Docket No.: SON-2960
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Akira YAEGASHI

Art Unit: N/A

Application No.: Not Yet Assigned

Filed: March 26, 2004

For: IMAGE TRANSMISSION SYSTEM, IMAGE PICKUP APPARATUS, IMAGE PICKUP APPARATUS UNIT, KEY GENERATING APPARATUS, AND PROGRAM

CLAIM FOR PRIORITY AND SUBMISSION OF DOCUMENTS

MS Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby claims priority under 35 U.S.C. 119 based on the following prior foreign application filed in the following foreign country on the date indicated:

Country	Application No.	Date
Japan	P2003-101783	April 4, 2003

In support of this claim, a certified copy of the said original foreign application is filed herewith.

Dated: March 26, 2004

Respectfully submitted,

By _____ Robert S. Green Reg. No. 41,800

Ronald P. Kananen
Registration No.: 24,104

Rader, Fishman & Grauer PLLC
Suite 501
1233 20th Street, N.W.
Washington, D.C. 20036
Telephone: (202) 955-3750
Facsimile: (202) 955-3751
Customer No.: 23353

504P042800500

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

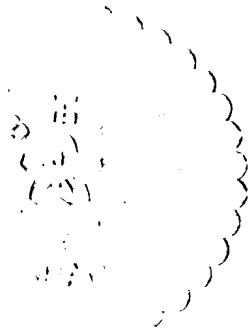
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　４月　４日

出願番号
Application Number: 特願２００３－１０１７８３

[ST. 10/C]: [ＪＰ２００３－１０１７８３]

出願人
Applicant(s): ソニー株式会社



２００４年　２月　３日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００４－３００５３４４

【書類名】　特許願
【整理番号】　0390074707
【提出日】　平成15年 4月 4日
【あて先】　特許庁長官　太田　信一郎　殿
【国際特許分類】　H04L　9/00
G09C　1/00
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　八重樫　章
【特許出願人】
【識別番号】　000002185
【氏名又は名称】　ソニー株式会社
【代理人】
【識別番号】　100095957
【弁理士】
【氏名又は名称】　亀谷　美明
【電話番号】　03-5919-3808
【選任した代理人】
【識別番号】　100096389
【弁理士】
【氏名又は名称】　金本　哲男
【電話番号】　03-3226-6631
【選任した代理人】
【識別番号】　100101557
【弁理士】
【氏名又は名称】　萩原　康司
【電話番号】　03-3226-6631

【手数料の表示】

【予納台帳番号】　040224

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0012374

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　画像伝送システム，撮像装置，撮像装置ユニット，鍵生成装置，およびプログラム

【特許請求の範囲】

【請求項１】　ネットワークを介して画像を伝送する画像伝送システムであって，

各々が固有の識別番号を有し，撮像した画像を暗号化して前記ネットワークに伝送するための暗号化機能を有する１または２以上の撮像装置と，

前記画像を暗号化するための暗号化キーおよび前記暗号化された画像を復号化するための復号化キーを前記撮像装置ごとに生成する鍵生成装置と，

前記復号化キーと前記撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体と，

前記リムーバブル記録媒体が接続され，前記復号化キーを用いて前記暗号化された画像を復号化する復号化機能を有し，前記ネットワークを介して前記撮像装置が伝送する画像を閲覧するための閲覧装置と，

前記閲覧装置からアクセス可能な前記撮像装置の認証を行う認証サーバと，

を含むことを特徴とする，画像伝送システム。

【請求項２】　ネットワークを介して画像を伝送する画像伝送システムであって，

各々が固有の識別番号を有する１または２以上の撮像装置と，

前記撮像装置が撮像した画像を暗号化して前記ネットワークに伝送するとともに，前記暗号化された画像の復号化するための復号化キーを生成する鍵生成装置と，

前記復号化キーと前記撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体と，

前記リムーバブル記録媒体が接続され，前記復号化キーを用いて前記暗号化された画像を復号化する復号化機能を有し，前記ネットワークを介して前記撮像装置が伝送する画像を閲覧するための閲覧装置と，

前記閲覧装置からアクセス可能な前記撮像装置の認証を行う認証サーバと，

を含むことを特徴とする，画像伝送システム。

【請求項３】　ネットワークを介して画像を伝送する画像伝送システムであって，

各々が固有の識別番号を有する１または２以上の撮像装置と，

前記撮像装置が撮像した画像を暗号化して前記ネットワークに伝送する伝送装置と，

前記画像を暗号化するための暗号化キーおよび前記暗号化された画像を復号化するための復号化キーを前記撮像装置ごとに生成する鍵生成装置と，

前記復号化キーと前記撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体と，

前記リムーバブル記録媒体が接続され，前記復号化キーを用いて前記暗号化された画像を復号化する復号化機能を有し，前記ネットワークを介して前記撮像装置が伝送する画像を閲覧するための閲覧装置と，

前記閲覧装置からアクセス可能な前記撮像装置の認証を行う認証サーバと，

を含むことを特徴とする，画像伝送システム。

【請求項４】　ネットワークを介して画像を伝送する画像伝送システムであって，

各々が固有の識別番号を有し，撮像した画像を暗号化して前記ネットワークに伝送するための暗号化機能を有する１または２以上の撮像装置と，

前記撮像装置が画像を暗号化するための暗号化キーおよび復号化キーを前記撮像装置ごとに生成する鍵生成装置と，

前記復号化キーと前記撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体と，

前記リムーバブル記録媒体が接続され，前記復号化キーを用いて前記暗号化された画像を復号化する復号化機能を有し，前記ネットワークを介して前記撮像装置が伝送する画像を閲覧するための閲覧装置と，

を含むことを特徴とする，画像伝送システム。

【請求項５】　ネットワークを介して画像を伝送する画像伝送システムに用いられる撮像装置であって，

固有の識別番号を記録する記録部と，

撮像した画像を暗号化する暗号化部と，

前記暗号化された画像をネットワークに伝送する通信部と，

を備えたことを特徴とする，撮像装置。

【請求項６】　前記通信部は，前記画像を暗号化するための暗号化キーを鍵生成装置から受信する受信部を含むことを特徴とする，請求項５に記載の撮像装置。

【請求項７】　前記通信部は，ＵＳＢポートを含むことを特徴とする，請求項５に記載の撮像装置。

【請求項８】　前記記録手段は，ＩＰアドレスを記録することを特徴とする，請求項５に記載の撮像装置。

【請求項９】　固有の識別番号を有し，撮像した画像を暗号化してネットワークに伝送するための暗号化機能を有する撮像装置と，

前記撮像装置が暗号化した画像を復号化するための復号化キーと前記撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体と，

を含むことを特徴とする，撮像装置ユニット。

【請求項１０】　前記撮像装置は，前記画像を暗号化するための暗号化キーを鍵生成装置から受信することを特徴とする，請求項９に記載の撮像装置ユニット。

【請求項１１】　前記リムーバブル記録媒体は，前記画像を復号化するための復号化キーを鍵生成装置から受信することを特徴とする，請求項９に記載の撮像装置ユニット。

【請求項１２】　前記撮像装置は，ＵＳＢカメラであることを特徴とする，請求項９に記載の撮像装置ユニット。

【請求項１３】　前記撮像装置は，ＩＰカメラであることを特徴とする，請求項９に記載の撮像装置ユニット。

【請求項１４】　ネットワークを介して画像を伝送する際の暗号処理に用いられる暗号化キーおよび復号化キーを生成する鍵生成装置であって，

固有の識別番号を有し，撮像した画像を暗号化してネットワークに伝送するた

めの暗号化機能を有する撮像装置に対して，前記画像を暗号化するための暗号化キーを生成して送出するとともに，

前記暗号化された画像を復号化するための復号化キーを生成して，前記復号化キーと前記撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体に送出することを特徴とする，鍵生成装置。

【請求項１５】　前記撮像装置を前記ネットワークに中継する中継機能を有することを特徴とする，請求項１４に記載の鍵生成装置。

【請求項１６】　前記撮像装置が撮像した画像を圧縮する圧縮機能を有することを特徴とする，請求項１４に記載の鍵生成装置。

【請求項１７】　コンピュータを，請求項１４に記載の鍵生成装置として機能させるためのプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は画像伝送システムおよびその関連技術にかかり，特に，家庭やオフィス内の監視を行うセキュリティサービスに利用可能な画像伝送システム，撮像装置，撮像装置ユニット，鍵生成装置，およびプログラムに関する。

【０００２】

【従来の技術】

近年におけるネットワーク技術の発展にはめざましいものがあり，ネットワークを介して様々な情報のやりとりが可能な環境が整っている。このような中で，家庭やオフィス内にカメラを設置し，カメラからの映像や静止画などをネットワークを介して伝送することで，遠隔地から家庭やオフィス内の様子を監視する監視システムがある（例えば，特許文献１参照。）。このような監視システムは，家庭やオフィスの防犯のほか，留守中のペットを監視したり，遠隔地に住む一人暮らしの老人の様子を確認したりといった様々な利用法がある。

【０００３】

【特許文献１】

特開２００２－１８３８６０

【０００４】

【発明が解決しようとする課題】

上述のように，ネットワークを介して様々な情報のやりとりが可能な環境が整ってきたことにともない，ネットワークにおけるセキュリティ確保の問題が顕在化しつつある。すなわち，ネットワークを介して様々な情報を容易にやりとりできる反面，その情報は，悪意を持った第三者から盗聴されるという危険を常に抱えている。このような問題は，プライバシー保護の観点からも近年クローズアップされつつあり，その対策が急務である。

【０００５】

また，上述の監視システムでは，家庭やオフィスと監視会社とを専用線で結ぶことでセキュリティ確保を図るシステムも採用されている。しかしながら，かかる専用線によるシステムは費用が非常に掛かるため，大規模な企業やオフィスビル，あるいは美術館など，セキュリティ確保に十分な費用を掛けられる一部でのみ採用されているのが現状である。このような背景から，一般の家庭では監視カメラを用いた監視システムを気軽に利用できるまでには至っていない。

【０００６】

また，近年における携帯電話などの携帯端末の普及に伴って発展した新たな監視システムとして，家庭内に設置した監視カメラとユーザが外出時に携帯する携帯端末とを，家庭内に設置したルータなどを用いて仮想施設網（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ：ＶＰＮ）構成とするシステムがある。ＶＰＮによれば，送信側および受信側のそれぞれに暗号処理機能を持たせることで，専用線を引くのと実質的に同様の効果がある。しかしながら，例えば仕事の合間に一時的に家庭内を確認したい場合や専用のモニタを用いて常時監視したい場合など，携帯端末からではなく，コンピュータから監視カメラを確認したいという要請があるが，オフィス内のＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）からでは，ＶＰＮに接続することが不可能である。

【０００７】

本発明は，従来の監視システムおよび画像伝送システムが有する上記問題点に鑑みてなされたものであり，本発明の目的は，監視目的の画像やモニタリング画

像など他者に見られたくない画像をネットワーク経由で送出するにあたり，他者に見られることなく，本人のみが安全に，ネットワークを介して画像を見ることの可能な，新規かつ改良された画像伝送システム，撮像装置，撮像装置ユニット，鍵生成装置，およびプログラムを提供することである。

【０００８】

【課題を解決するための手段】

上記課題を解決するため，本発明の第１の観点によれば，ネットワークを介して画像を伝送する画像伝送システムが提供される。本発明の画像伝送システムは，少なくとも以下の構成要素を含むことを特徴とする。

・各々が固有の識別番号を有し，撮像した画像を暗号化してネットワークに伝送するための暗号化機能を有する１または２以上の撮像装置

・画像を暗号化するための暗号化キーおよび暗号化された画像を復号化するための復号化キーを撮像装置ごとに生成する鍵生成装置

・復号化キーと撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体

・リムーバブル記録媒体が接続され，復号化キーを用いて暗号化された画像を復号化する復号化機能を有し，ネットワークを介して撮像装置が伝送する画像を閲覧するための閲覧装置

・閲覧装置からアクセス可能な撮像装置の認証を行う認証サーバ

【０００９】

かかる画像伝送システムによれば，撮像装置に，画像の暗号化を行う機能を有するようにしたことで，撮像装置内で画像に暗号処理を施すことができ，セキュリティを高めることができる。そして，撮像装置からの画像をネットワークに送出するにあたり，画像を暗号処理した後，ネットワークに送出するようにした。そして，ネットワークに送出された画像は，本人のみが所有するリムーバブル記録媒体を用いて本人認証を行った後でなければ，復号化して見ることができない。かかるシステムの実現のため，撮像装置は，各々が固有の識別番号を有している。このようにして，ネットワーク上では画像が暗号化されているため，本人のみが安全に，ネットワークを介して画像を見ることができる。

【００１０】

上記課題を解決するため，本発明の第２の観点によれば，ネットワークを介して画像を伝送する画像伝送システムが提供される。本発明の画像伝送システムは，少なくとも以下の構成要素を含むことを特徴とする。

・各々が固有の識別番号を有する１または２以上の撮像装置

・撮像装置が撮像した画像を暗号化してネットワークに伝送するとともに，暗号化された画像の復号化するための復号化キーを生成する鍵生成装置

・復号化キーと撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体

・リムーバブル記録媒体が接続され，復号化キーを用いて暗号化された画像を復号化する復号化機能を有し，ネットワークを介して撮像装置が伝送する画像を閲覧するための閲覧装置

・閲覧装置からアクセス可能な撮像装置の認証を行う認証サーバ

【００１１】

かかる画像伝送システムによれば，鍵生成装置に，画像の暗号化を行う機能を有するようにしたことで，撮像装置が設置された家庭やオフィス内で画像に暗号処理を施すことができ，セキュリティを高めることができる。そして，撮像装置からの画像をネットワークに送出するにあたり，画像を暗号処理した後，ネットワークに送出するようにした。そして，ネットワークに送出された画像は，本人のみが所有するリムーバブル記録媒体を用いて本人認証を行った後でなければ，復号化して見ることができない。かかるシステムの実現のため，撮像装置は，各々が固有の識別番号を有している。このようにして，ネットワーク上では画像が暗号化されているため，本人のみが安全に，ネットワークを介して画像を見ることができる。

【００１２】

上記課題を解決するため，本発明の第３の観点によれば，ネットワークを介して画像を伝送する画像伝送システムが提供される。本発明の画像伝送システムは，少なくとも以下の構成要素を含むことを特徴とする。

・各々が固有の識別番号を有する１または２以上の撮像装置

・撮像装置が撮像した画像を暗号化してネットワークに伝送する伝送装置
・画像を暗号化するための暗号化キーおよび暗号化された画像を復号化するための復号化キーを撮像装置ごとに生成する鍵生成装置
・復号化キーと撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体
・リムーバブル記録媒体が接続され，復号化キーを用いて暗号化された画像を復号化する復号化機能を有し，ネットワークを介して撮像装置が伝送する画像を閲覧するための閲覧装置
・閲覧装置からアクセス可能な撮像装置の認証を行う認証サーバ

【００１３】

かかる画像伝送システムによれば，撮像装置が撮像した画像を暗号化してネットワークに伝送する伝送装置と，画像を暗号化するための暗号化キーおよび暗号化された画像を復号化するための復号化キーを撮像装置ごとに生成する鍵生成装置を別個のシステム構成要素としている。そして，伝送装置に，画像の暗号化を行う機能を有するようにしたことで，撮像装置が設置された家庭やオフィス内で画像に暗号処理を施すことができ，セキュリティを高めることができる。そして，撮像装置からの画像をネットワークに送出するにあたり，画像を暗号処理した後，ネットワークに送出するようにした。そして，ネットワークに送出された画像は，本人のみが所有するリムーバブル記録媒体を用いて本人認証を行った後でなければ，復号化して見ることができない。かかるシステムの実現のため，撮像装置は，各々が固有の識別番号を有している。このようにして，ネットワーク上では画像が暗号化されているため，本人のみが安全に，ネットワークを介して画像を見ることができる。

【００１４】

上記課題を解決するため，本発明の第４の観点によれば，ネットワークを介して画像を伝送する画像伝送システムが提供される。本発明の画像伝送システムは，少なくとも以下の構成要素を含むことを特徴とする。
・各々が固有の識別番号を有し，撮像した画像を暗号化してネットワークに伝送するための暗号化機能を有する１または２以上の撮像装置

・撮像装置が画像を暗号化するための暗号化キーおよび復号化キーを撮像装置ごとに生成する鍵生成装置

・復号化キーと撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体

・リムーバブル記録媒体が接続され，復号化キーを用いて暗号化された画像を復号化する復号化機能を有し，ネットワークを介して撮像装置が伝送する画像を閲覧するための閲覧装置

【００１５】

かかる画像伝送システムによれば，閲覧装置からアクセス可能な撮像装置の認証を行う認証サーバをシステム構成要素としなくても，上記第１の観点にかかる画像伝送システムと同様の効果を得ることができる。すなわち，認証サーバによる管理を行わなくても，撮像装置に，画像の暗号化を行う機能を有するようにしたことで，撮像装置内で画像に暗号処理を施すことができ，撮像装置単体であっても十分にセキュリティを高めることができる。

【００１６】

また，上記課題を解決するため，本発明の第５の観点によれば，ネットワークを介して画像を伝送する画像伝送システムに用いられる撮像装置が提供される。本発明の撮像装置は，少なくとも以下の構成要素を備えたことを特徴とする。

・固有の識別番号を記録する記録部

・撮像した画像を暗号化する暗号化部

・暗号化された画像をネットワークに伝送する通信部

【００１７】

かかる撮像装置によれば，画像の暗号化を行う暗号化部を備えるようにしたことで，撮像装置内で画像に暗号処理を施すことができ，セキュリティを高めることができる。そして，撮像装置からの画像をネットワークに送出するにあたり，画像を暗号化部で暗号処理した後，通信部からネットワークに送出するようにした。そして，ネットワークに送出された画像は，本人認証を行った後でなければ，復号化して見ることができない。かかるシステムの実現のため，撮像装置は，固有の識別番号を記録部に記録している。このようにして，ネットワーク上では

画像が暗号化されているため，本人のみが安全に，ネットワークを介して画像を見ることができる。

【００１８】

本発明の撮像装置において，以下のような応用が可能である。

【００１９】

通信部が，画像を暗号化するための暗号化キーを鍵生成装置から受信する受信部を含むようにすれば，撮像装置内に暗号化キーを保持しておく必要がなくなり，記憶部の容量を縮小することができる。また，暗号化キーを保持しないため，セキュリティを高めるのにも有効である。

【００２０】

また，本発明の撮像装置は，通信部（インタフェース）がＵＳＢポートを含む，いわゆるＵＳＢカメラであってもよい。ＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）は，シリアル・インタフェイス規格であり，機器の接続を自動的に認識するプラグ・アンド・プレイ機能や，接続するコンピュータやルータ装置などの電源を入れたままコネクタの抜き差しができるホット・プラグ機能を備えている。また，コンピュータやルータ装置から機器への電源供給も可能である。また，ほとんどのコンピュータやルータ装置などに接続が可能である。このような点で，通信部（インタフェース）がＵＳＢポートを含む，いわゆるＵＳＢカメラであると，利便性が極めて高い。

【００２１】

また，撮像装置は，記録手段にＩＰアドレスを記録した，いわゆるＩＰカメラであってもよい。ＩＰカメラであれば，１０／１００ＢａｓｅのＬＡＮ網（イーサネットポート）に接続するだけで、追加のハードウェアを購入することなくネットワーク６００上のどのコンピュータからでもアクセスすることができる。

【００２２】

また，上記課題を解決するため，本発明の第６の観点によれば，固有の識別番号を有し，撮像した画像を暗号化してネットワークに伝送するための暗号化機能を有する撮像装置と，撮像装置が暗号化した画像を復号化するための復号化キーと撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体と，を含む

ことを特徴とする，撮像装置ユニットが提供される。

【００２３】

かかる撮像装置ユニットによれば，撮像装置に，画像の暗号化を行う機能を有するようにしたことで，撮像装置内で画像に暗号処理を施すことができ，セキュリティを高めることができる。そして，撮像装置からの画像をネットワークに送出するにあたり，画像を暗号処理した後，ネットワークに送出するようにした。そして，ネットワークに送出された画像は，本人のみが所有するリムーバブル記録媒体を用いて本人認証を行った後でなければ，復号化して見ることができない。かかるシステムの実現のため，撮像装置は，各々が固有の識別番号を有している。このようにして，ネットワーク上では画像が暗号化されているため，本人のみが安全に，ネットワークを介して画像を見ることができる。

【００２４】

本発明の撮像装置ユニットにおいて，以下のような応用が可能である。

【００２５】

撮像装置が，画像を暗号化するための暗号化キーを鍵生成装置から受信するようにすれば，撮像装置内に暗号化キーを保持しておく必要がなくなり，記憶部の容量を縮小することができる。また，暗号化キーを保持しないため，セキュリティを高めるのにも有効である。

【００２６】

また，リムーバブル記録媒体についても，画像を復号化するための復号化キーを鍵生成装置から受信するようにしてもよい。この場合，暗号化キーを生成する鍵生成装置と復号化キーを生成する鍵生成装置が，同じ鍵生成装置であってもよく，異なる鍵生成装置であってもよい。

【００２７】

また，撮像装置は，上記本発明の第５の観点と同様に，ＵＳＢカメラとしたり，ＩＰカメラとしたりすることができる。

【００２８】

また，本発明の第７の観点によれば，ネットワークを介して画像を伝送する際の暗号処理に用いられる暗号化キーおよび復号化キーを生成する鍵生成装置が提

供される。本発明の鍵生成装置は，固有の識別番号を有し，撮像した画像を暗号化してネットワークに伝送するための暗号化機能を有する撮像装置に対して，画像を暗号化するための暗号化キーを生成して送出するとともに，暗号化された画像を復号化するための復号化キーを生成して，復号化キーと撮像装置の識別番号とを関連付けて記録するリムーバブル記録媒体に送出することを特徴とする。

【００２９】

かかる鍵生成装置によれば，撮像装置が，撮像装置内に暗号化キーを保持しておく必要がなくなり，撮像装置の記憶部の容量を縮小することができる。また，撮像装置が暗号化キーを保持しないため，セキュリティを高めるのにも有効である。

【００３０】

本発明の撮像装置ユニットにおいて，以下のような応用が可能である。

【００３１】

撮像装置をネットワークに中継する中継機能を有するものとすることが可能である。いわゆるルータ装置を鍵生成装置として機能させることができる。

【００３２】

また，撮像装置が撮像した画像を圧縮する圧縮機能を有することも可能である。ネットワークに送出する画像のサイズを縮小化することにより，処理速度を向上させることができる。また，撮像装置に必ずしも圧縮機能を搭載する必要がなくなるため，撮像装置の小型化・低価格化を図ることができる。

【００３３】

また，本発明の第８の観点によれば，コンピュータを，上記第７の観点にかかる鍵生成装置として機能させるためのプログラムが提供される。ここで，プログラムはいかなるプログラム言語により記述されていてもよい。また，そのプログラムを記録した，コンピュータにより読み取り可能な記録媒体としては，例えば，ＣＤ－ＲＯＭ，ＤＶＤ－ＲＯＭ，フロッピーディスク（ＦＤ：Ｆｌｏｐｐｙ Ｄｉｓｋ）など，プログラムを記録可能な記録媒体として現在一般に用いられている記録媒体，あるいは将来用いられるいかなる記録媒体をも採用することができる。

【００３４】

【発明の実施の形態】

以下に添付図面を参照しながら，本発明にかかる画像伝送システム，撮像装置，撮像装置ユニット，鍵生成装置，およびプログラムの好適な実施の形態について詳細に説明する。なお，本明細書及び図面において，実質的に同一の機能構成を有する構成要素については，同一の符号を付することにより重複説明を省略する。

【００３５】

（第１の実施の形態）

図１は，本実施の形態にかかる画像伝送システム１０のシステム構成の概略を示す説明図である。なお，図１において括弧書きで示した参照符号は，後述の第２の実施の形態において説明する。本実施の形態にかかる画像伝送システム１０について，図１を参照しながら説明する。

【００３６】

画像伝送システム１０は，図１に示したように，撮像装置１００と，鍵生成装置２００と，メモリーカード３００と，閲覧装置４００と，認証サーバ５００を含んで構成され，ネットワーク６００を介して画像を伝送するシステムである。

【００３７】

なお，図１において，ネットワーク６００は，多数の情報ネットワークを相互に接続することによって世界中に広がったネットワーク環境，例えば，公衆回線網を利用したインターネットを想定している。また，図１には，説明の便宜上，各構成要素を１つずつ示しているが，撮像装置１００および鍵生成装置２００に相当する構成要素は，一般家庭やオフィスなどに１つまたは２つ以上設置されるものであり，ネットワーク６００に極めて多数（例えば，数十万台の規模で）接続されるものである。また，リムーバブル記憶媒体３００に相当する構成要素は，撮像装置１００と実質的に同数程度存在するものである。また，閲覧装置４００に相当する構成要素は，ネットワーク６００に接続される任意のコンピュータや携帯電話などであり，ネットワーク６００に極めて多数（例えば，数千万台の規模で）接続されるものである。また，認証サーバ５００に相当する構成要素は

ネットワーク６００に複数接続されていてもよい。

【００３８】

また，本実施の形態において「画像」とは，撮像装置１００が撮像対象を光学的あるいは音声的に捉え，ディジタル化することにより得られたディジタルデータをいい，撮像装置１００がネットワーク６００を介して伝送可能なＡＶ（Ａｕｄｉｏ－Ｖｉｄｅｏ）情報である。撮像装置１００の機能に応じて，動画（映像），静止画（画像），音声，文字情報など，あるいはこれらの任意の組み合わせをいうものとする。また，撮像装置１００が画像を得ることを「撮像」という。

【００３９】

以下に，本実施の形態にかかる画像伝送システム１０の各構成要素について詳細に説明する。

【００４０】

（撮像装置１００）

撮像装置１００は，今後家庭やオフィス内に広く普及されると予測される，防犯やペットの監視などに用いられるセキュリティカメラを想定している。すなわち，セキュリティカメラを遠隔地からモニタリングする場合に，画像をネットワーク６００を介して送出すると，他者からのぞき見られる可能性がある。本実施の形態では，かかるセキュリティカメラの画像を安全にネットワーク上から，どこからでも本人（あるいは本人の承諾を得た者）のみが見られる仕組みについて説明する。

【００４１】

本実施の形態では，撮像装置１００の一例として，ＵＳＢカメラ１１０と，ＩＰカメラ１２０を例に挙げて説明する。なお，ＵＳＢカメラ１１０とＩＰカメラ１２０を区別する必要がないときには，単に撮像装置１００という。

【００４２】

ＵＳＢカメラ１１０は，コンピュータ用の周辺機器としてＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）接続可能なカメラである。ＵＳＢは，シリアル・インタフェイス規格であり，機器の接続を自動的に認識するプラグ・アンド・プレイ機能や，接続するコンピュータやルータ装置などの電源を入れたままコ

ネクタの抜き差しができるホット・プラグ機能を備えている。また，コンピュータやルータ装置から機器への電源供給も可能である。そして，ほとんどのコンピュータやルータ装置などに接続が可能である。

【００４３】

また，ＩＰカメラ１２０は，ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）を利用したカメラである。ＩＰカメラ１２０は，ＩＰアドレスを有しており，１０／１００ＢａｓｅのＬＡＮ網（イーサネットポート）に接続するだけで、追加のハードウェアを購入することなくネットワーク６００上のどのコンピュータからでもアクセスすることができる。

【００４４】

図２は，ＩＰカメラ１２０の概略構成を示す説明図である。

ＩＰカメラ１２０は，図２に示したように，記録部１２２と，暗号化部１２４と，インタフェース１２６と，画像処理部１２８を備えている。

【００４５】

記録部１２２は，少なくともこのＩＰカメラ１２０の固有の識別番号１３０を記録している。また記録部１２２は，ＩＰカメラとして機能させるためのＩＰアドレス１３２を記録している。さらに記録部１２２は，後述の鍵生成装置２００から伝送され，受信部１３８で受信した暗号化キー１３４を記録する。記録部１２２は，これら識別番号１３０，ＩＰアドレス１３２，および暗号化キー１３４を必要に応じて書き換え（更新）可能なように，例えば，電気的に内容を書き換えることができるＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）であるフラッシュメモリーで構成することができる。

【００４６】

暗号化部１２４は，このＩＰカメラ１２０が撮像し，画像処理部１２８で所定の処理が行われた画像を暗号化する。画像の暗号化には，記録部１２２に記録された暗号化キー１３４が用いられる。暗号化方式としては，良く知られた秘密鍵方式（共通鍵方式とも称される）や公開鍵方式などがあるが，本実施の形態では，暗号化キーと復号化キーを同一のキーとする秘密鍵方式を採用することができる。暗号処理を行うための暗号化キーは，後述の鍵生成装置２００から送信され

る。

【００４７】

インタフェース１２６は，主に暗号化された画像をネットワーク６００に伝送する送信部１３６と，鍵生成装置２００から伝送される暗号化キー１３４を受信する受信部１３８とからなる。なお，送信部１３６と受信部１３８は，共通のポートであってもよい。また，送信部１３６または受信部１３８の規格はどのようなものであってもよい。例えば，受信部１３８は，ＵＳＢポートであってもよい。

【００４８】

本実施の形態にかかる撮像装置１００は，上述のように，記録部１２２と，暗号化部１２４と，インタフェース１２６に特徴を有するものである。撮像装置１００の不図示および未説明の構成については，どのようなものであってもよい。

【００４９】

撮像装置１００は，家庭やオフィスなどに１台または２台以上設置される。撮像装置１００は，外部からアクセス可能なように，各々が固有の識別番号を有している。例えば，ＵＳＢカメラ１１０の識別番号を「＃１」，ＩＰカメラ１２０の識別番号を「＃２」などのように，固有の識別番号がシリアルにあるいはランダムに割り振られている。

【００５０】

（鍵生成装置２００）

再び図１を参照しながら説明すると，鍵生成装置２００は，上述の撮像装置１００をネットワーク６００に接続する機能を有するとともに，撮像装置１００が暗号処理を行うための暗号化キーおよび暗号化された画像を復号化するための復号化キーを撮像装置１００ごとに生成する装置である。また，本実施の形態では，鍵生成装置２００は，撮像装置１００からの画像をネットワーク６００に伝送するための伝送装置としても機能する。

【００５１】

本実施の形態では，鍵生成装置２００の一例として，コンピュータ２１０と，ルータ２２０を例に挙げて説明する。なお，コンピュータ２１０とルータ２２０

を区別する必要がないときには，単に鍵生成装置２００という。

【００５２】

コンピュータ２１０は，デスクトップ型のものでもノート型（ラップトップ型）のものでもよく，あるいはパーム型のＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ）と称されるものであってもよい。上述のＵＳＢカメラ１１０はコンピュータ２１０のＵＳＢ端子に接続可能である。

【００５３】

コンピュータ２１０は，撮像装置１００が暗号処理を行うための暗号化キーおよび暗号化された画像を復号化するための復号化キーを生成する機能を有する。かかる機能の実現のため，例えば，コンピュータ２１０には暗号化キーおよび復号化キーを生成するためのアプリケーションソフトが組み込まれる。かかるアプリケーションソフトは，暗号化キーおよび復号化キーを生成するためのコンピュータプログラムを記録した記録媒体から読み込まれる。

【００５４】

ルータ２２０は，ＬＡＮ同士やＬＡＮとＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）を相互に接続するための装置である。ルータ２２０は，ＯＳＩ基本参照モデルのネットワーク層で，パケット中継処理をする。ＴＣＰ／ＩＰネットワークでは，ＩＰアドレス（ＩＰ：Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）を見て中継経路の制御を行う。データ・リンク層では隣接ノード間もしくは同一セグメント上でしかデータの伝達ができないが，ルータ２００はデータ・リンク層でのデータ転送機能を組み合わせて，ネットワーク６００上のあらゆるノード間同士でデータを転送する。上述のＩＰカメラ１２０はルータ２２０のイーサネットポートに接続可能である。

【００５５】

ルータ２２０は，撮像装置１００が暗号処理を行うための暗号化キーおよび暗号化された画像を復号化するための復号化キーを生成する機能を有する。かかる機能は，ルータ２２０にハードウェア的に組み込まれていてもよい。あるいは，かかる機能の実現のため，例えば，ルータ２２０には暗号化キーおよび復号化キーを生成するためのアプリケーションソフトが組み込まれる。かかるアプリケー

ションソフトは，暗号化キーおよび復号化キーを生成するためのコンピュータプログラムを記録した記録媒体から読み込まれる。

【００５６】

鍵生成装置２００は，暗号化キーを撮像装置１００に送信するとともに，復号化キーを撮像装置１００の識別番号と関連付けて，後述のメモリーカード３００に記録する。このための手段として，鍵生成装置２００は，少なくとも，暗号化キーおよび復号化キーを撮像装置１００あるいはメモリーカード３００に送信するための送信手段を有している。復号化キーをメモリーカード３００に送信するための送信手段の一例として，例えば，メモリーカード３００用のカードスロットを設けることも可能である。

【００５７】

また，鍵生成装置２００には，撮像装置１００の識別番号が登録される。このための手段として，鍵生成装置２００は，少なくとも，撮像装置１００の識別番号の登録を受けるための受信手段と，撮像装置１００の識別番号を保持するための記憶手段とを有している。鍵生成装置２００は，撮像装置１００から送信された識別番号を，ネットワーク６００を介して後述の認証サーバ５００に送信する。

【００５８】

また，鍵生成装置２００は，画像圧縮機能を有するようにしてもよい。鍵生成装置２００には，通常のＭＰＥＧ４のエンコーダに搭載されるようなマイクロプロセッサ（Ｄｉｇｉｔａｌ　Ｓｉｇｎａｌ　Ｐｒｏｃｅｓｓｏｒ：ＤＳＰ）を搭載することができる。すなわち，撮像装置１００が撮像した画像は，鍵生成装置２００を介してネットワーク６００に送出される。この際，鍵生成装置２００は，撮像装置１００が圧縮した画像を圧縮した後，ネットワーク６００に送出する。これは，後述するように，画像を閲覧するための閲覧装置４００について，比較的処理能力の小さい携帯電話なども想定しており，データ量の大きな画像を処理するのが難しい場合を想定したものである。

【００５９】

あるいは，鍵生成装置２００はネットワーク６００に対し，例えば，まず静止

画を送出し，その後に動画（映像）を送出するようにしてもよい。データ量の小さな静止画をいち早く送出することで，撮像装置１００が撮像した情報をユーザにいち早く知らせることができる。例えばユーザ宅への侵入者が撮像装置１００や鍵生成装置２００が設置されているのに気付いてこれらを壊そうとした場合でも，静止画であれば瞬時に送出することができるので，防犯に役立つという利点もある。

【００６０】

（メモリーカード３００）

リムーバブル記憶媒体の一例たるメモリーカード３００は，ユーザが後述の閲覧装置４００を用いて，撮像装置１００から伝送される画像を閲覧するために用いられるものである。すなわち，ユーザが閲覧装置４００を用いて撮像装置１００から伝送させる画像を閲覧する際，メモリーカード３００を閲覧装置４００に接続し，メモリーカード３００に記録された認証情報を用いてユーザ認証を行う。このようにして，撮像装置１００から伝送される画像を，認証された本人のみが閲覧することができる。以下に，メモリーカード３００について説明する。

【００６１】

メモリーカード３００は，鍵生成装置２００が生成した復号化キーと，撮像装置１００の識別番号とを関連付けて記録する。１つのメモリーカード３００に，１つの撮像装置１００を対応付けてもよく，複数の撮像装置１００を対応付けてもよい。より具体的には，メモリーカード３００には，撮像装置１００の識別番号が１つまたは複数予め与えられており，復号化キーは後段階で与えることができる。また，メモリーカード３００には，このメモリーカード３００を使用するためのパスワードが設定されている。このような各種情報の保持および更新のために，メモリーカード３００は，記録内容を書き換え可能な手段で構成することができる。メモリーカード３００は，例えば，電気的に内容を書き換えることができるＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）であるフラッシュメモリーで構成することができる。

【００６２】

また，メモリーカード３００は，上述の鍵生成装置２００に接続して復号化キ

ーを受信するための接続手段，および，後述の閲覧装置４００に接続するための接続手段を有している。これら接続手段は同じものであってもよく，別個のものであってもよい。接続手段としては，例えば，ほとんどのコンピュータやルータ装置などに接続が可能なように，ＵＳＢコネクタで構成することができる。あるいは，上述の鍵生成装置あるいは後述の閲覧装置４００の側に，メモリーカード３００を読み書き可能な手段，例えば，カードスロットなどを設けるようにしてもよい。

【００６３】

以上説明したメモリーカード３００は，上述の撮像装置１００の付属的構成要素（オプション）として位置づけることができる。メモリーカード３００は，例えば，撮像装置１００と一緒に，撮像装置ユニットとして商取引の対象とすることが可能である。メモリーカード３００は，携帯に便利なように，例えばキーホルダー型，バッジ型，ペン型など様々な形状とすることができる。また，メモリーカード３００を他の所持品に固着可能なように，例えば磁石や吸盤などを備えることも可能である。

【００６４】

また，撮像装置１００およびメモリーカード３００を商取引の対象とするにあたり，撮像装置１００およびメモリーカード３００を一体にして，撮像装置ユニットとして商取引の対象としてもよい。あるいは，撮像装置１００のみをまず商取引の対象とし，メモリーカード３００は事後的にオプションとして商取引の対象としてもよい。

【００６５】

（閲覧装置４００）

閲覧装置４００は，ユーザが，撮像装置１００から伝送される画像を閲覧するために用いられるものである。すなわち，ユーザが撮像装置１００から伝送される画像を閲覧する際，上述のメモリーカード３００を閲覧装置４００に接続して，ユーザ認証を行う。そして，ユーザ認証を行った後，撮像装置１００から伝送される画像を閲覧することができる。以下に，閲覧装置４００について詳細に説明する。

【００６６】

本実施の形態では，閲覧装置４００の一例として，コンピュータ４１０と，携帯電話４２０を例に挙げて説明する。なお，コンピュータ４１０と携帯電話４２０を区別する必要がないときには，単に閲覧装置４００という。

【００６７】

コンピュータ４１０は，デスクトップ型のものでもノート型（ラップトップ型）のものでもよく，あるいはパーム型のＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ）と称されるものであってもよい。コンピュータ４１０には，ネットワーク６００に接続してＨＴＴＰ（ＨｙｐｅｒＴｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）ファイルを閲覧するためのソフト（ブラウザソフト）が組み込まれている。そして，ブラウザソフトには，撮像装置１００からの画像を閲覧するためのプラグインソフトが追加されている。このプラグインソフトによって，画像を閲覧するユーザがパスワードを入力するなどの各種操作を行うことができる。

【００６８】

コンピュータ４１０には，上述のメモリーカード３００の記録内容を読み出し可能な手段が設けられている。かかる手段としては，例えばメモリーカード３００がＵＳＢコネクタを備えている場合には，ＵＳＢポートとすることができる。また，メモリーカード３００がＵＳＢコネクタを備えていない場合に，コンピュータ４１０に，カードスロットを設けたり，外部接続機器としてカードリーダを接続したりすることが可能である。

【００６９】

携帯電話４２０は，少なくともネットワーク６００を介して画像の受信を行うことができる受信機能と，画像を表示可能な表示機能と，表示部に対する所定の操作を行うための操作部を備えている。その他の機能，例えば音声通話機能や音声や画像の記録機能などについてはどのようなものであってもよい。携帯電話４２０にも，上述のコンピュータ４１０に組み込まれるようなプラグインソフトが組み込まれており，画像を閲覧するユーザがパスワードを入力するなどの各種操作を行うことができる。

【００７０】

携帯電話４２０には，上述のメモリーカード３００の記録内容を読み出し可能な手段が設けられている。かかる手段としては，例えばメモリーカード３００がＵＳＢコネクタを備えている場合には，ＵＳＢポート，あるいはアダプタを介してＵＳＢコネクタを接続可能なポートとすることができる。また，メモリーカード３００がＵＳＢコネクタを備えていない場合に，携帯電話４２０にカードスロットを設けることも可能である。

【００７１】

（認証サーバ５００）

認証サーバ５００は，画像伝送システム１０において，システム内の認証処理を行うサーバである。すなわち，認証サーバ５００は，ユーザがメモリーカード３００を用いて閲覧装置４００において画像を閲覧する際に，ユーザ認証を行い，ユーザがアクセス可能な撮像装置１００を認証する。

【００７２】

また，認証サーバ５００の他の機能としては，撮像装置１００がネットワーク６００に対して送出する画像を保存することも可能である。撮像装置１００が監視カメラとして利用されている場合に，撮像装置１００の画像を保存することで，防犯に効果がある。この際，撮像装置１００からは静止画および動画（映像）を送ることができる。例えば上述のように，撮像装置１００からはまず静止画が送られてこれを認証サーバ５００に保存し，次いで，動画が送られて認証サーバ５００に保存することができる。

【００７３】

以上，図１を参照しながら，画像伝送システム１０の構成について説明した。

次いで，図３～図４を参照しながら，画像伝送システム１０の初期設定・登録時の動作について説明する。図３は，初期設定・登録時の動作をシステム構成とともに示す説明図であり，図４は，初期設定・登録時の動作を示す流れ図である。

【００７４】

①撮像装置１００および鍵生成装置２００の接続

まず，撮像装置１００（ＵＳＢカメラ１１０あるいはＩＰカメラ１２０）およびメモリーカード３００を鍵生成装置２００に接続する（ステップＳ１０１）。ＵＳＢカメラ１１０の場合には鍵生成装置２００にＵＳＢ接続され，ＩＰカメラ１２０の場合には鍵生成装置２００にＩＰ接続される。また，メモリーカード３００は鍵生成装置２００にＵＳＢ接続される。

【００７５】

②撮像装置１００から鍵生成装置２００に対する識別番号の送信

次いで，撮像装置１００が鍵生成装置２００に対し，識別番号を送信する。鍵生成装置２００は，撮像装置１００から識別番号の送信を受けて，撮像装置１００の識別番号を登録する（ステップＳ１０２）。

【００７６】

③鍵生成装置２００による暗号化キーおよび復号化キーの生成

鍵生成装置２００は，撮像装置１００ごとに固有の暗号化キーおよび復号化キーを生成する（ステップＳ１０３）。例えば，鍵生成装置２００にＵＳＢカメラ１１０とＩＰカメラ１２０が接続されている場合には，ＵＳＢカメラ１１０とＩＰカメラ１２０のそれぞれに固有の識別番号を生成する。暗号化方式として秘密鍵方式（共通鍵方式）を採用する場合には，暗号化キーと復号化キーを同一のものとすることができる。

【００７７】

④鍵生成装置２００による暗号化キーおよび復号化キーの送信

鍵生成装置２００は，撮像装置１００に対し，撮像装置１００ごとに生成された暗号化キーを記録する。撮像装置１００において，暗号化キーは，主記憶装置内に暗号化されて記録される。さらに，鍵生成装置２００は，メモリーカード３００に対し，復号化キーを記録する（ステップＳ１０４）。

【００７８】

⑤鍵生成装置２００による認証サーバ５００に対する識別番号の送信

さらに本実施の形態では，鍵生成装置２００は，ネットワーク６００を介して認証サーバ５００に対し，撮像装置１００の識別番号を登録する（ステップＳ１０５）。

【００７９】

なお，以上説明した初期設定・登録は，撮像装置１００およびメモリーカード３００の製造時に製造業者（メーカ）が行ったり，あるいは，撮像装置１００およびメモリーカード３００の販売時に販売業者（小売店など）が行ってもよい。この場合，事後的に，パスワードの変更や暗号化キー・復号化キーの変更を行えるようにすることがセキュリティ上好ましい。

【００８０】

以上，図３～図４を参照しながら，初期設定・登録時の動作について説明した。

次いで，図５～図６を参照しながら，画像伝送システム１０における画像の閲覧時の動作について説明する。図５は，画像の閲覧時の動作をシステム構成とともに示す説明図であり，図６は，画像の閲覧時の動作を示す流れ図である。

【００８１】

①撮像装置１００による撮像

上述のように，撮像装置１００は，家庭やオフィス内に設置されて，防犯やペットの監視などに用いられるセキュリティカメラを想定している。初期設定・登録が行われた撮像装置１００は，家庭やオフィス内に設置されて，家庭やオフィス内の画像を撮像する。撮像された画像は，撮像装置１００内で暗号化されて，ネットワークに送出される（ステップＳ２０１）。

【００８２】

②閲覧装置４００から認証サーバ５００に認証要求

次いで，撮像装置１００が撮像した画像をユーザが遠隔地から閲覧する動作について説明する。閲覧を行うユーザは，上述のメモリーカード３００を所持している。このユーザは，遠隔地に設置されたコンピュータ４１０あるいは所持している携帯電話４２０などの閲覧装置４００から，まず認証サーバ５００にアクセスする。この際，ユーザＩＤやパスワードなどを入力する。閲覧装置４００は，認証サーバ５００に対し，このユーザの認証要求を行うとともに，ユーザがアクセス可能な撮像装置１００の認証要求を行う（ステップＳ２０２）。

【００８３】

③認証サーバ５００が撮像装置１００を認証

閲覧装置４００からの撮像装置１００の認証要求を受けて，認証サーバ５００は，ユーザの認証を行うとともに，撮像装置１００の認証を行う（ステップＳ２０３）。このようにして，閲覧装置４００から撮像装置１００の閲覧の準備が完了する。

【００８４】

④閲覧装置４００がメモリーカード３００を検出

認証サーバ５００により撮像装置１００が認証されると，ユーザは，メモリーカード３００を閲覧装置４００に接続する。なお，ユーザおよび撮像装置１００の認証よりも前の段階で，メモリーカード３００を閲覧装置４００に接続してもよい。そして，閲覧装置４００は，メモリーカード３００を検出する（ステップＳ２０４）。

【００８５】

⑤閲覧装置４００が，メモリーカード３００の識別番号と撮像装置１００の識別番号との照合

閲覧装置４００は，メモリーカード３００を検出すると，メモリーカード３００に記録された撮像装置１００の識別番号と，認証サーバ５００により認証され，画像の伝送を受けようとする撮像装置１００の識別番号とを照合する（ステップＳ２０５）。

【００８６】

⑥復号化キーの取得

メモリーカード３００に記録された撮像装置１００の識別番号と，画像の伝送を受けようとする撮像装置１００の識別番号とが一致すると，閲覧装置４００は，メモリーカード３００から復号化キーを取得する。そして，閲覧装置４００は，その復号化キーを用いて，撮像装置１００から伝送される暗号化された画像を復号化する（ステップＳ２０６）。

【００８７】

⑦閲覧装置４００での画像の閲覧

以上の一連の工程を経て，ユーザは，閲覧装置４００での画像の閲覧が可能と

なる（ステップＳ２０７）。

【００８８】

（第１の実施の形態の効果）

以上説明したように，本実施の形態によれば，撮像装置１００に，画像の暗号化を行う機能を有するようにしたことで，撮像装置１００内で画像に暗号処理を施すことができ，セキュリティを高めることができる。

【００８９】

また，撮像装置１００からの画像をネットワーク６００に送出するにあたり，画像を暗号化部１２４で暗号処理した後，ネットワーク６００に送出するようにした。そして，ネットワーク６００に送出された画像は，本人のみが所有するメモリーカード３００を用いて本人認証を行った後でなければ，復号化して見ることができない。このようにして，ネットワーク６００上では画像が暗号化されているため，本人のみが安全に，ネットワーク６００を介して画像を見ることができる。

【００９０】

また，閲覧装置４００で閲覧するにあたり，暗号化された画像の復号化キーをメモリーカード３００に記録し，このメモリーカード３００を使用するためのパスワードを設定している。このため，メモリーカード３００を盗難あるいは紛失するなどした場合であっても，悪意ある第三者によるメモリーカード３００の不正使用を防止することができる。

【００９１】

（第２の実施の形態）

上記第１の実施の形態にかかる画像閲覧システム１０は，撮像装置１００で画像を暗号化するものであった。本実施の形態では，撮像装置１００で画像を暗号化する代わりに，鍵生成装置２００で画像を暗号化するシステムについて説明する。

【００９２】

本実施の形態にかかる画像伝送システム２０のシステム構成の概略は，図１に示したものと実質的に同様であるので，重複説明を省略する。なお，図１におい

て，本実施の形態にかかるシステム構成要素を，括弧書き符号で示している。

【００９３】

本実施の形態では，撮像装置１００は暗号化機能を備えていない。撮像装置１０１の一例として，図７に示したＩＰカメラ１２０’を例に挙げて説明する。なお，上記第１の実施の形態と同様の構成要素については，同一の参照番号を付すことで重複説明を省略する。図７に示した本実施の形態のＩＰカメラ１２０は，図２に示したＩＰカメラ１２０と対比して，暗号化部１２４と受信部１３８に相当する構成要素を必須の構成要素としない。そして，記録部１２２は，暗号化キー１３４を記録していない。すなわち，本実施の形態では，撮像装置１００において，画像の撮像のみを行い，撮像した画像の暗号化は行わない。

【００９４】

本実施の形態では，撮像装置１００から鍵生成装置２００に対して，暗号化されていない画像が送出される。そして，鍵生成装置２００は，撮像装置１００から送出された画像を暗号化する。鍵生成装置２００の暗号化機能については，上記第１の実施の形態で説明した，撮像装置１００の暗号化部１２４と実質的に同様のものとすることができる。

【００９５】

次いで，図８～図９を参照しながら，画像伝送システム２０の初期設定・登録時の動作について説明する。図８は，初期設定・登録時の動作をシステム構成とともに示す説明図であり，図９は，初期設定・登録時の動作を示す流れ図である。

【００９６】

上記第１の実施の形態との相違点についてのみ説明する。

本実施の形態では，鍵生成装置２００は，撮像装置１００に対して暗号化キーを渡す動作を行わない。すなわち，図８に示したように，図３に示した「④暗号化キー」の動作が行われない。また，図９に示したように，図４に示したステップＳ１０４は，鍵生成サーバ２００がメモリーカード３００に対し復号化キーを記録する（ステップＳ１０４’）という動作に置き換わる。この動作以外については，上記第１の実施の形態と実質的に同様である。

【００９７】

次いで，図１０～図１１を参照しながら，画像伝送システム２０における画像の閲覧時の動作について説明する。図１０は，画像の閲覧時の動作をシステム構成とともに示す説明図であり，図１１は，画像の閲覧時の動作を示す流れ図である。

【００９８】

上記第１の実施の形態との相違点についてのみ説明する。

図１０には，鍵生成装置２００を示している。そして，①撮像装置１００で撮像された画像は，鍵生成装置２００において暗号化される。また，図１１に示したように，図６に示したステップＳ２０１は，撮像装置１００による撮像，鍵生成装置２００による画像の暗号化（ステップＳ２０１’）という動作に置き換わる。この動作以外については，上記第１の実施の形態と実質的に同様である。

【００９９】

（第２の実施の形態の効果）

以上説明したように，本実施の形態によれば，鍵生成装置２００に，画像の暗号化を行う機能を有するようにしたことで，上記第１の実施の形態と実質的に同様の効果を得ることが可能である。

【０１００】

さらに，撮像装置１００内に暗号化部を備える必要がないので，装置規模を縮小することができる。また，撮像装置１００内に暗号化キーを保持しておく必要がなくなり，記憶部の容量を縮小することができる。また，撮像装置１００内に暗号化キーを保持しないため，セキュリティを高めるのにも有効である。

【０１０１】

（第３の実施の形態）

上記第２の実施の形態にかかる画像閲覧システム２０は，撮像装置１００で画像を暗号化する代わりに，鍵生成装置２００で画像を暗号化するものであった。そして，第２の実施の形態にかかる鍵生成装置２００は，撮像装置１００をネットワーク６００に接続する手段と，暗号化キーおよび復号化キーを生成する手段とを兼ねたシステム構成要素である。本実施の形態では，撮像装置１００をネッ

トワーク６００に接続する手段と，暗号化キーおよび復号化キーを生成する手段とを別個の独立した構成要素としたシステムについて説明する。

【０１０２】

図１２は，本実施の形態にかかる画像伝送システム３０のシステム構成の概略を示す説明図である。本実施の形態にかかる画像伝送システム３０について，図８を参照しながら説明する。

【０１０３】

画像伝送システム３０は，図１２に示したように，第２の実施の形態にかかる画像伝送システム２０と比較して，鍵生成装置２００と伝送装置２５０とを別個の装置して構成したものである。

【０１０４】

本実施の形態にかかる鍵生成装置２００は，画像を暗号化するための暗号化キーおよび暗号化された画像を復号化するための復号化キーを生成する機能を有する。かかる機能の実現のため，例えば，鍵生成装置２００には暗号化キーおよび復号化キーを生成するためのアプリケーションソフトが組み込まれる。かかるアプリケーションソフトは，暗号化キーおよび復号化キーを生成するためのコンピュータプログラムを記録した記録媒体から読み込まれる。

【０１０５】

また，鍵生成装置２００は，暗号化キーを撮像装置１００に送信するとともに，復号化キーを撮像装置１００の識別番号と関連付けて，メモリーカード３００に記録する。このための手段として，鍵生成装置２００は，少なくとも，暗号化キーおよび復号化キーを撮像装置１００あるいはメモリーカード３００に送信するための送信手段を有している。復号化キーをメモリーカード３００に送信するための送信手段の一例として，例えば，メモリーカード３００用のカードスロットを設けることも可能である。

【０１０６】

また，鍵生成装置２００には，撮像装置１００の識別番号が登録される。このための手段として，鍵生成装置２００は，少なくとも，撮像装置１００の識別番号の登録を受けるための受信手段と，撮像装置１００の識別番号を保持するため

の記憶手段とを有している。鍵生成装置２００は，撮像装置１００から送信された識別番号を，ネットワーク６００を介して認証サーバ５００に送信する。

【０１０７】

一方，本実施の形態にかかる伝送装置２５０は，撮像装置１００が撮像した画像を暗号化して前記ネットワークに伝送する。伝送装置２５０は，画像圧縮機能を有するようにしてもよい。伝送装置２５０には，通常のＭＰＥＧ４のエンコーダに搭載されるようなマイクロプロセッサ（Ｄｉｇｉｔａｌ　Ｓｉｇｎａｌ　Ｐｒｏｃｅｓｓｏｒ：ＤＳＰ）を搭載することができる。

【０１０８】

画像伝送システム３０の初期設定・登録時の動作，および，画像の閲覧時の動作については，上記第２の実施の形態と実質的に同様であるので，重複説明を省略する。

【０１０９】

（第３の実施の形態の効果）

以上説明したように，本実施の形態によれば，撮像装置１００が撮像した画像を暗号化してネットワーク６００に伝送する伝送装置２５０と，画像を暗号化するための暗号化キーおよび前記暗号化された画像を復号化するための復号化キーを撮像装置１００ごとに生成する鍵生成装置２００を別個のシステム構成要素とすることで，上記第２の実施の形態と実質的に同様の効果を得ることが可能である。

【０１１０】

（第４の実施の形態）

上記第１の実施の形態にかかる画像閲覧システム１０は，システム構成要素として認証サーバ５００を含むものであった。本実施の形態では，システム構成要素として認証サーバ５００を含まないシステムについて説明する。

【０１１１】

図１３は，本実施の形態にかかる画像伝送システム２０のシステム構成の概略を示す説明図である。本実施の形態にかかる画像伝送システム２０について，図８を参照しながら説明する。

【０１１２】

画像伝送システム４０は，図１３に示したように，第１の実施の形態にかかる画像伝送システム１０と比較して，認証サーバ５００を含むことなく構成されたシステムである。

【０１１３】

次いで，図１４～図１５を参照しながら，画像伝送システム４０の初期設定・登録時の動作について説明する。図１４は，初期設定・登録時の動作をシステム構成とともに示す説明図であり，図１５は，初期設定・登録時の動作を示す流れ図である。

【０１１４】

上記第１の実施の形態との相違点についてのみ説明する。

本実施の形態では，①撮像装置１００および鍵生成装置２００の接続動作（ステップＳ１０１），②撮像装置１００から鍵生成装置２００に対する識別番号の送信，鍵生成装置２００による撮像装置１００の識別番号の登録動作（ステップＳ１０２），③鍵生成装置２００による暗号化キーおよび復号化キーの生成動作（ステップＳ１０３），④鍵生成装置２００による暗号化キーおよび復号化キーの送信動作（ステップＳ１０４）については，上記第１の実施の形態と実質的に同様である。

【０１１５】

本実施の形態では，鍵生成装置２００は，認証サーバ５００に対して撮像装置１００の識別番号を登録する動作を行わない。すなわち，鍵生成装置２００が，撮像装置１００に対し暗号化キーを，メモリーカード３００に復号化キーを記録する動作（ステップＳ１０４）を以て，初期設定・登録時の動作は終了する。

【０１１６】

次いで，図１６～図１７を参照しながら，画像伝送システム４０における画像の閲覧時の動作について説明する。図１６は，画像の閲覧時の動作をシステム構成とともに示す説明図であり，図１７は，画像の閲覧時の動作を示す流れ図である。

【０１１７】

上記第１の実施の形態との相違点についてのみ説明する。

本実施の形態では，認証サーバ５００をシステム構成要素として含まない。その結果として，閲覧装置４００による認証サーバ５００に対する認証要求は行われず，認証サーバ５００による撮像装置１００の認証も行われない。すなわち，図１６に示したように，図１に示した「②認証サーバ５００に対する認証要求」，および，「③認証サーバ５００による撮像装置１００の認証」の動作が行われない。また，図１７に示したように，図２に示したステップＳ２０２およびステップＳ２０３は行われない。この動作以外については，上記第１の実施の形態と実質的に同様である。

【０１１８】

（第４の実施の形態の効果）

以上説明したように，本実施の形態によれば，第１の実施の形態にかかる認証サーバ５００をシステム構成要素としなくても，上記第１の実施の形態と実質的に同様の効果を得ることができる。このため，撮像装置１００とメモリーカード３００とを組み合わせた撮像装置ユニットがあれば，認証サーバ５００による管理の必要がなく，上記第１の実施の形態と実質的に同様の効果を得ることができる。

【０１１９】

以上，添付図面を参照しながら本発明にかかる画像伝送システム，撮像装置，撮像装置ユニット，鍵生成装置，およびプログラムの好適な実施形態について説明したが，本発明はかかる例に限定されない。当業者であれば，特許請求の範囲に記載された技術的思想の範疇内において各種の変更例または修正例に想到し得ることは明らかであり，それらについても当然に本発明の技術的範囲に属するものと了解される。

【０１２０】

例えば，上記実施の形態では，メモリーカード３００を使用するためのパスワードを設定することで，メモリーカード３００を盗難あるいは紛失するなどした場合であっても，悪意ある第三者によるメモリーカード３００の不正使用を防止することができる点について説明した。しかしながら，パスワードを所定期間以

上にわたって固定しておくことは，セキュリティ上好ましくない。そこで，パスワードを定期的に書き換え可能なようにしてもよい。例えば，メモリーカード３００を閲覧装置４００に接続するたびごとに，パスワードの変更を確認するようにしてもよい。

【０１２１】

あるいは，メモリーカード３００を閲覧装置４００に接続するたびごとに，認証サーバ５００がワンタイムパスワード（使い捨てパスワード，ダイナミックパスワードとも称される。）を発行し，これを用いて閲覧を行うようにしてもよい。ワンタイムパスワードは，利用者が使うたびにデータが変わるパスワードである。パスワードが第三者に漏れても，固定的なパスワードのように繰り返して使うことができないので，安全性が極めて高い。例えば，上記実施の形態のように，画像伝送システムをホームセキュリティサービスに用いる場合，画像を長時間見続けるということは希である。そこで，１つのワンタイムパスワードで閲覧できる時間を例えば３０分などのように設定しておくことができる。仮にメモリーカード３００を紛失等し，悪意ある第三者が入手した場合でも，わずか１回３０分の閲覧しかできないので，被害を最小限にすることができる。ワンタイムパスワードは，閲覧装置４００で得るようにしてもよく，他の機器，例えば携帯電話やワンタイムパスワードを発行する専用モジュールから得るようにしてもよい。

【０１２２】

また，上記第４の実施の形態では，第１の実施の形態と比較して，システム構成要素として認証サーバ５００を含まないシステムについて説明した。第２の実施の形態および第３の実施の形態についても，同様に，認証サーバ５００を含まないシステムとすることも可能である。

【０１２３】

【発明の効果】

以上説明したように，本発明によれば，撮像装置に，画像の暗号化を行う機能を有するようにしたことで，撮像装置内で画像に暗号処理を施すことができ，セキュリティを高めることができる。そして，撮像装置からの画像をネットワークに送出するにあたり，画像を暗号処理した後，ネットワークに送出するようにし

た。そして，ネットワークに送出された画像は，本人のみが所有するリムーバブル記録媒体を用いて本人認証を行った後でなければ，復号化して見ることができない。かかるシステムの実現のため，撮像装置は，各々が固有の識別番号を有している。このようにして，ネットワーク上では画像が暗号化されているため，本人のみが安全に，ネットワークを介して画像を見ることができる。

【図面の簡単な説明】

【図１】

第１の実施の形態にかかる画像伝送システムの構成の一例を示す説明図である。

【図２】

第１の実施の形態にかかるＩＰカメラの構成を示す説明図である。

【図３】

第１の実施の形態にかかる初期設定・登録時の動作をシステム構成とともに示す説明図である。

【図４】

第１の実施の形態にかかる初期設定・登録時の動作を示す流れ図である。

【図５】

第１の実施の形態にかかる画像の閲覧時の動作をシステム構成とともに示す説明図である。

【図６】

第１の実施の形態にかかる画像の閲覧時の動作を示す流れ図である。

【図７】

第２の実施の形態にかかるＩＰカメラの構成を示す説明図である。

【図８】

第２の実施の形態にかかる初期設定・登録時の動作をシステム構成とともに示す説明図である。

【図９】

第２の実施の形態にかかる初期設定・登録時の動作を示す流れ図である。

【図１０】

第２の実施の形態にかかる画像の閲覧時の動作をシステム構成とともに示す説明図である。

【図１１】

第２の実施の形態にかかる画像の閲覧時の動作を示す流れ図である。

【図１２】

第３の実施の形態にかかる画像伝送システムの構成の一例を示す説明図である。

【図１３】

第４の実施の形態にかかる画像伝送システムの構成の一例を示す説明図である。

【図１４】

第４の実施の形態にかかる初期設定・登録時の動作をシステム構成とともに示す説明図である。

【図１５】

第４の実施の形態にかかる初期設定・登録時の動作を示す流れ図である。

【図１６】

第４の実施の形態にかかる画像の閲覧時の動作をシステム構成とともに示す説明図である。

【図１７】

第４の実施の形態にかかる画像の閲覧時の動作を示す流れ図である。

【符号の説明】

１０　画像伝送システム

１００　撮像装置

１１０　ＵＳＢカメラ

１２０　ＩＰカメラ

２００　鍵生成装置

２１０　コンピュータ

２２０　ルータ

３００　メモリーカード（リムーバブル記憶媒体）

４００　閲覧装置

４１０　コンピュータ

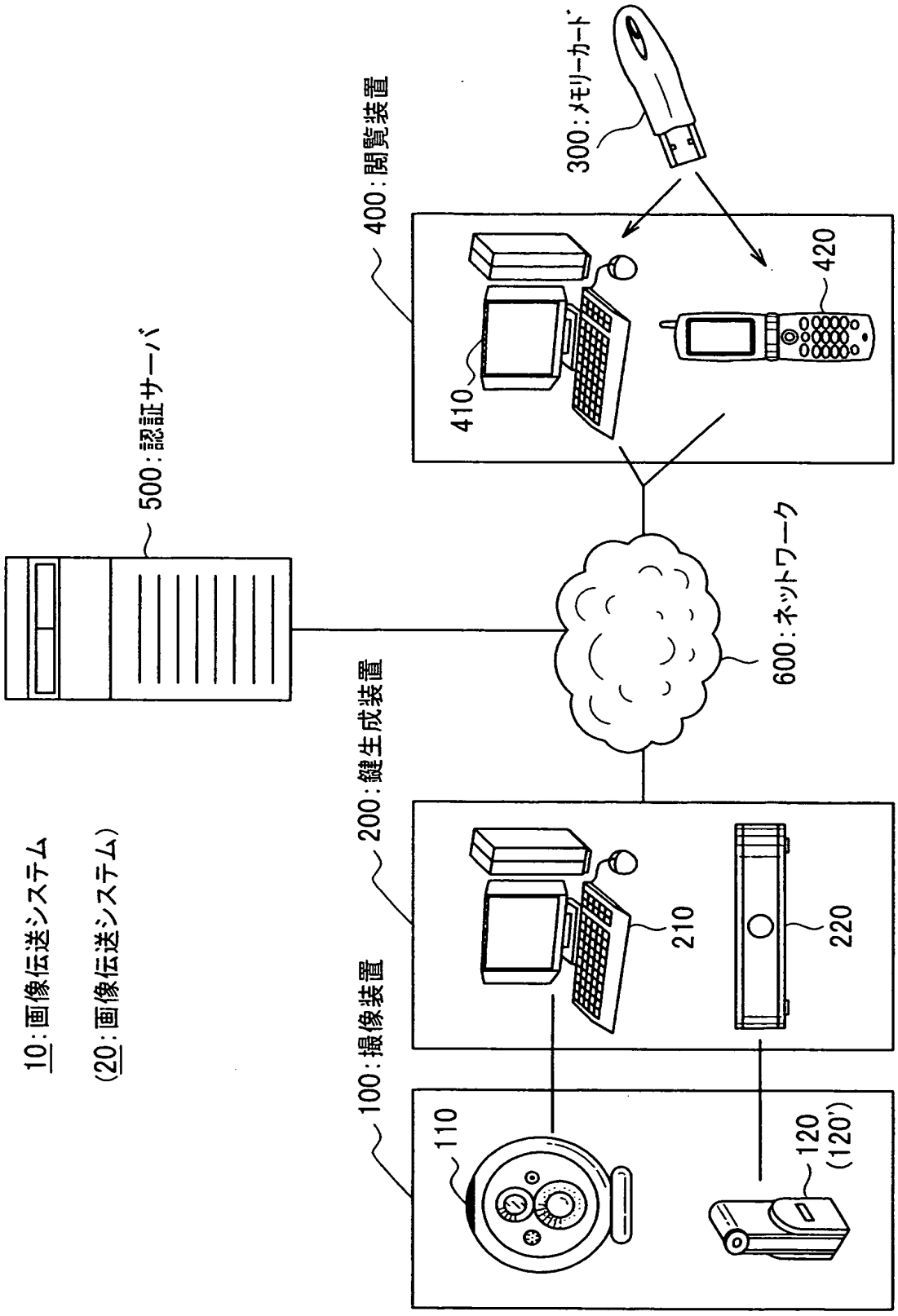
４２０　携帯電話

５００　認証サーバ

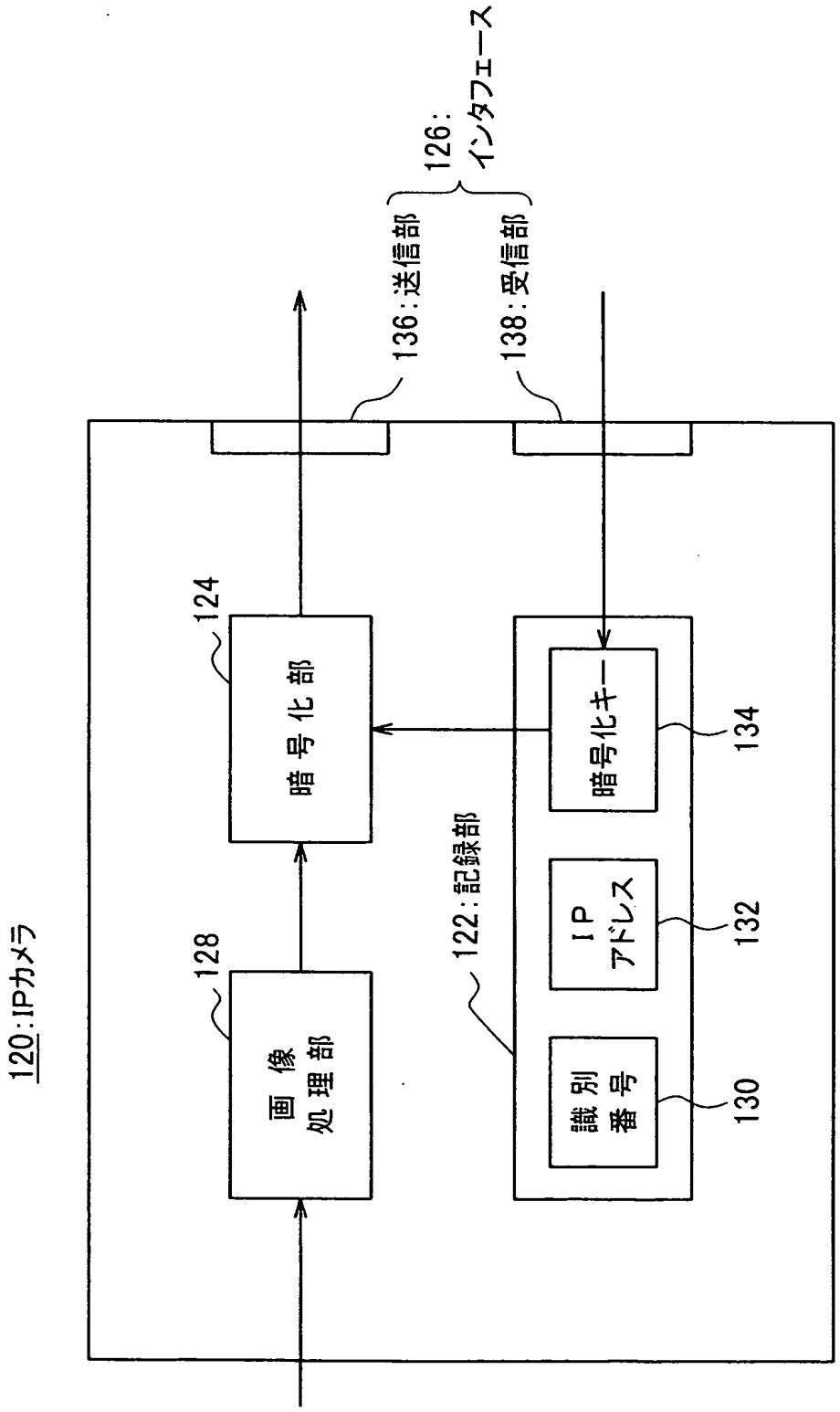
６００　ネットワーク

【書類名】　図面

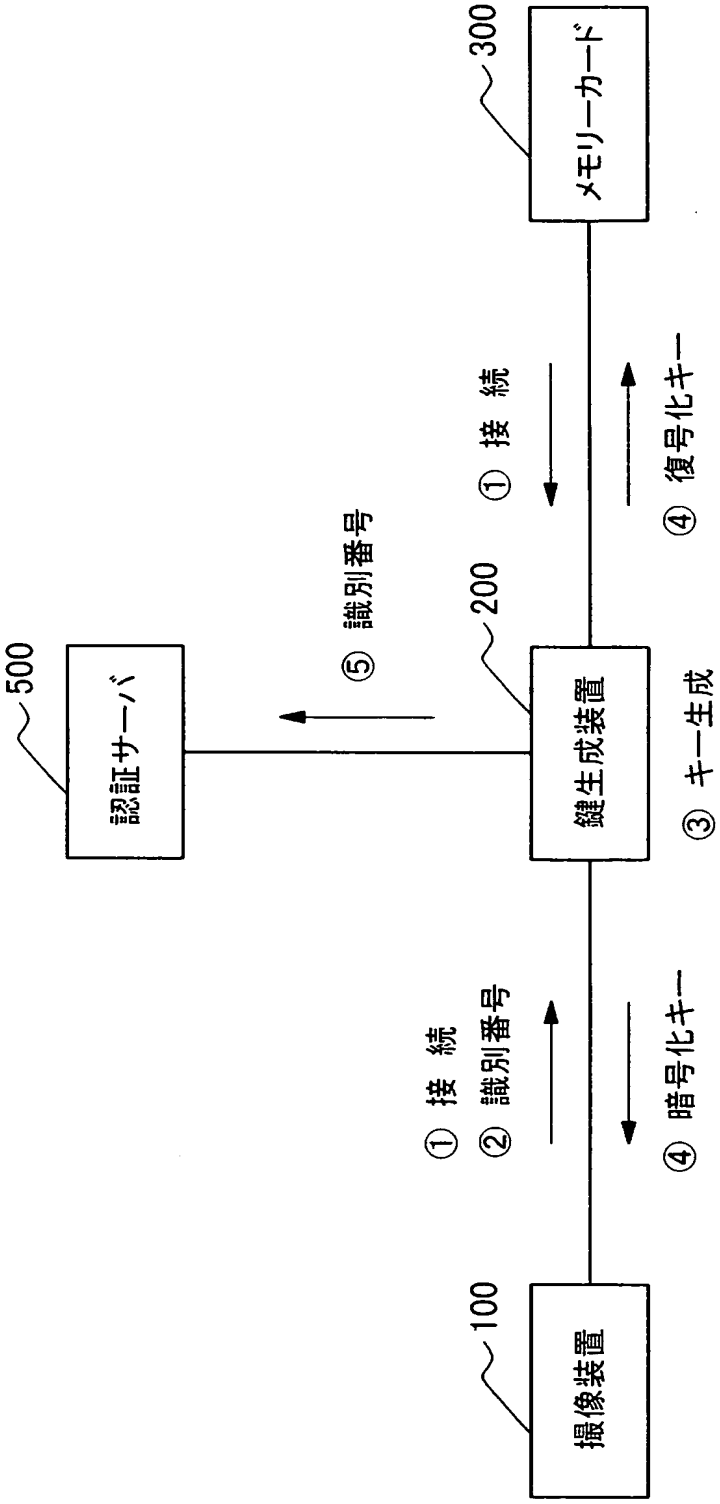
【図１】


10:画像伝送システム
(20:画像伝送システム)
500:認証サーバ
400:閲覧装置
300:メモリーカード
410
420
600:ネットワーク
200:鍵生成装置
210
220
100:撮像装置
110
120
(120')

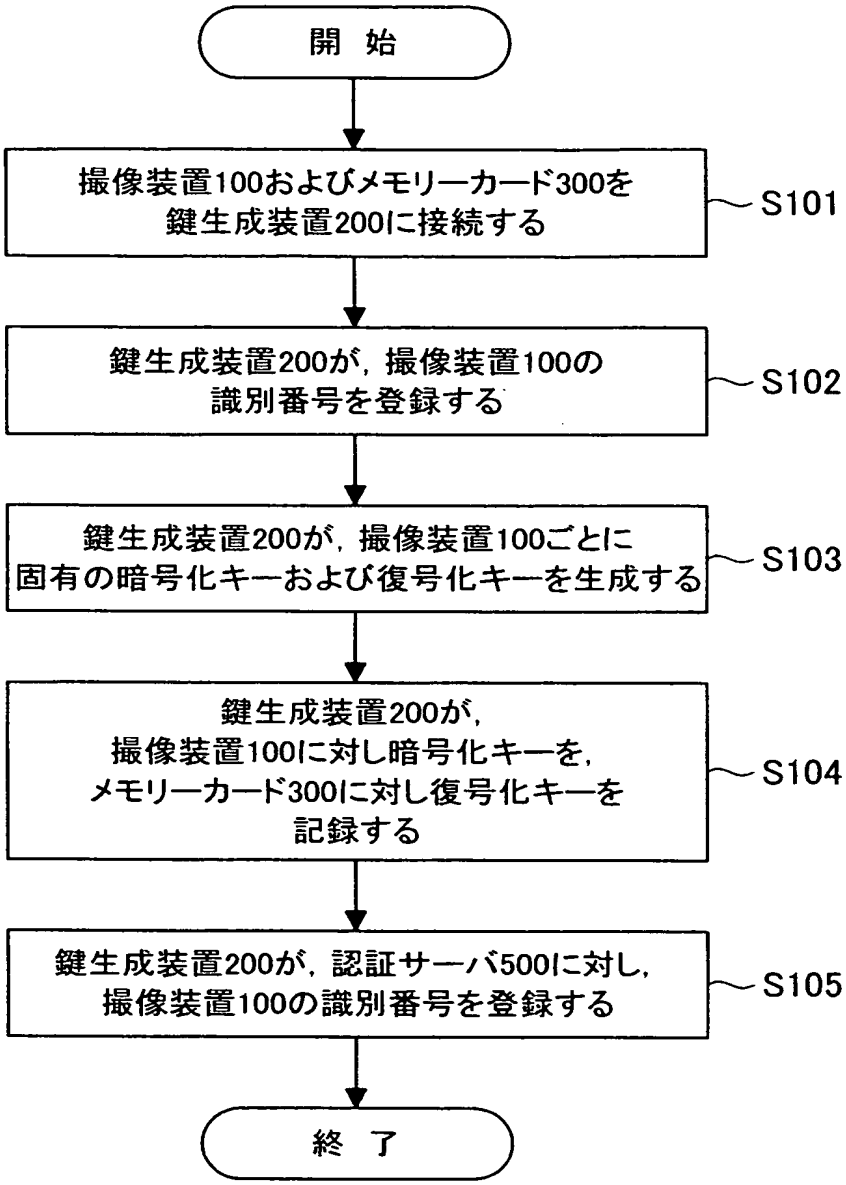
【図２】


120:IPカメラ
126:
インタフェース
136:送信部
138:受信部
124
暗号化部
128
画像
処理部
122:記録部
暗号化キー
134
IP
アドレス
132
識別
番号
130

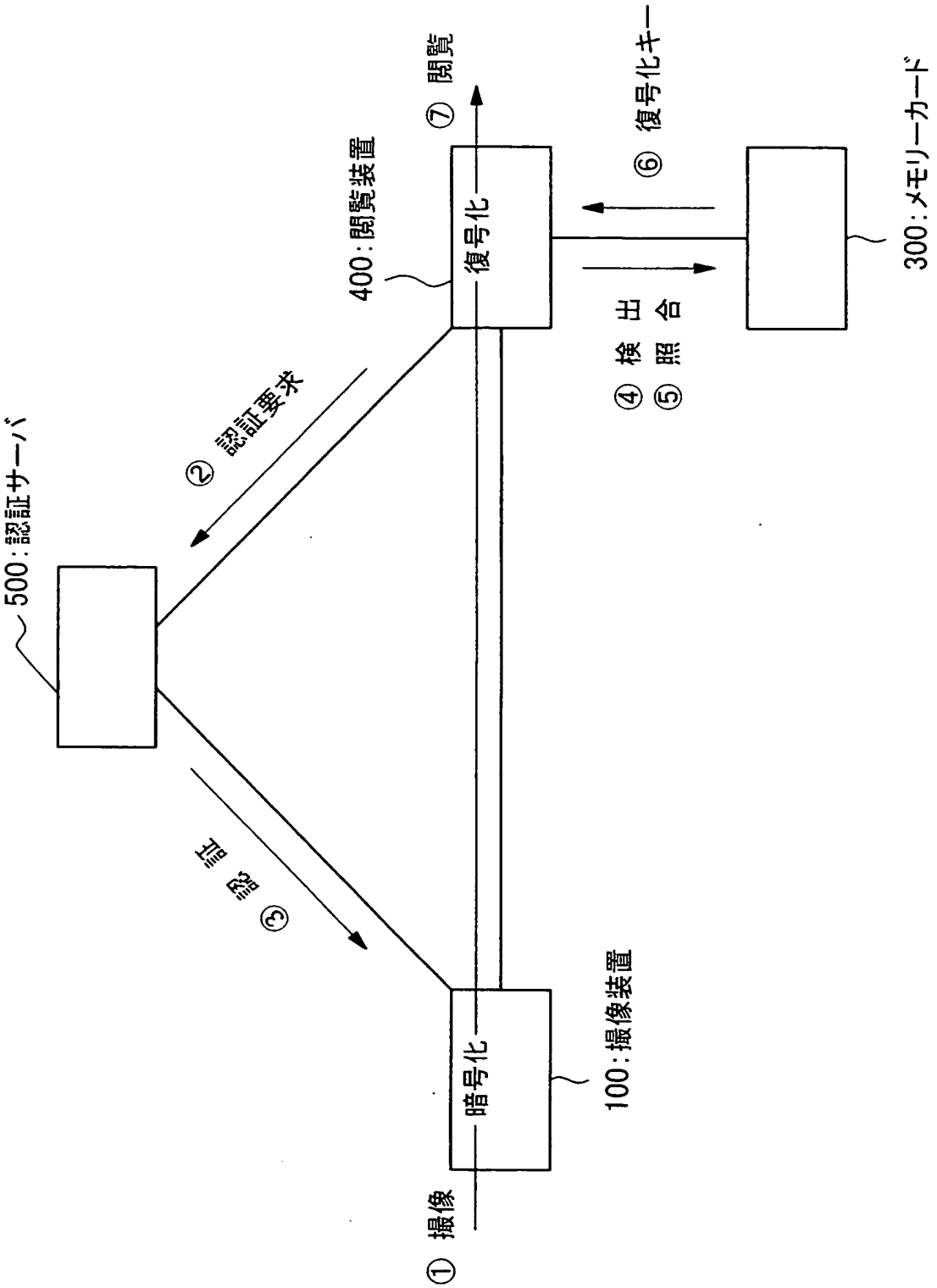
【図３】


300
メモリーカード
① 接 続
④ 復号化キー
200
鍵生成装置
③ キー生成
⑤ 識別番号
500
認証サーバ
① 接 続
② 識別番号
④ 暗号化キー
100
撮像装置

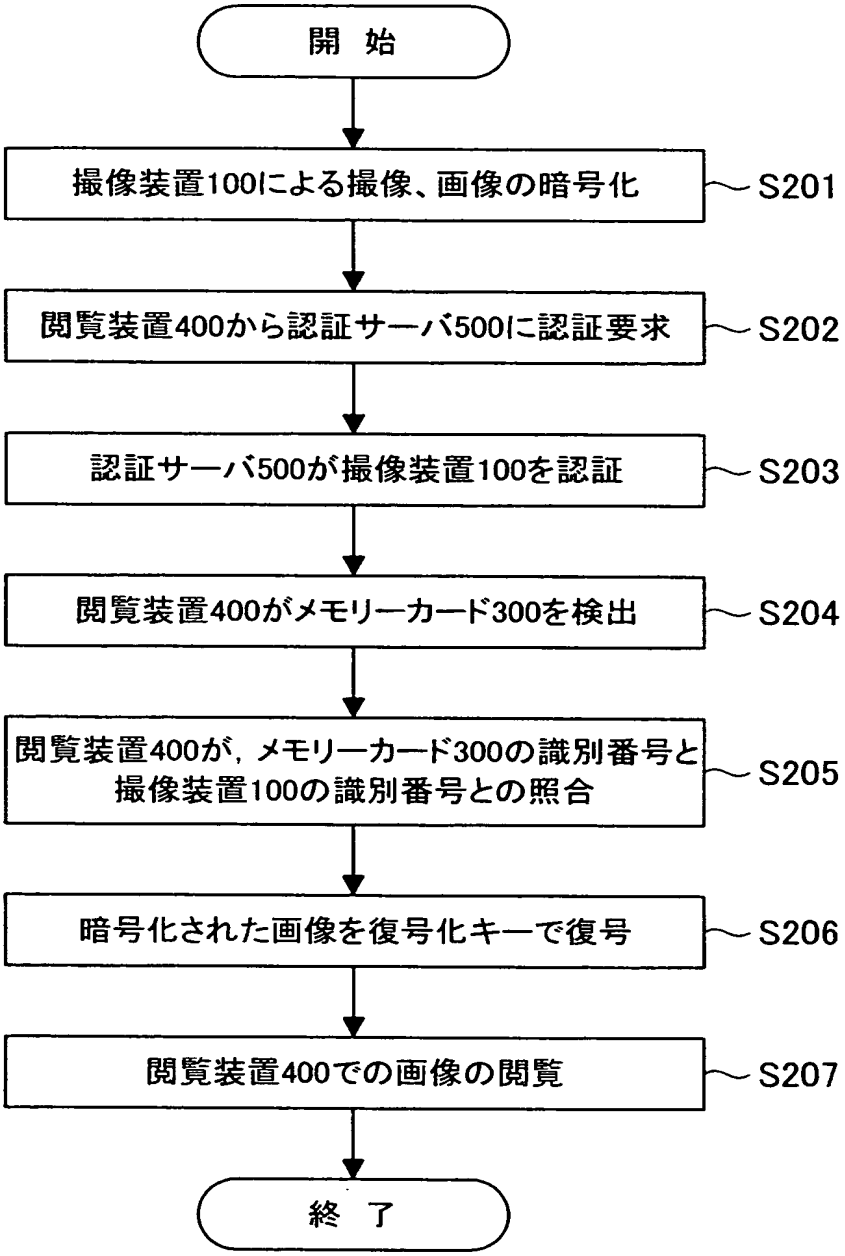
【図４】


開　始
撮像装置100およびメモリーカード300を
鍵生成装置200に接続する
S101
鍵生成装置200が，撮像装置100の
識別番号を登録する
S102
鍵生成装置200が，撮像装置100ごとに
固有の暗号化キーおよび復号化キーを生成する
S103
鍵生成装置200が，
撮像装置100に対し暗号化キーを，
メモリーカード300に対し復号化キーを
記録する
S104
鍵生成装置200が，認証サーバ500に対し，
撮像装置100の識別番号を登録する
S105
終　了

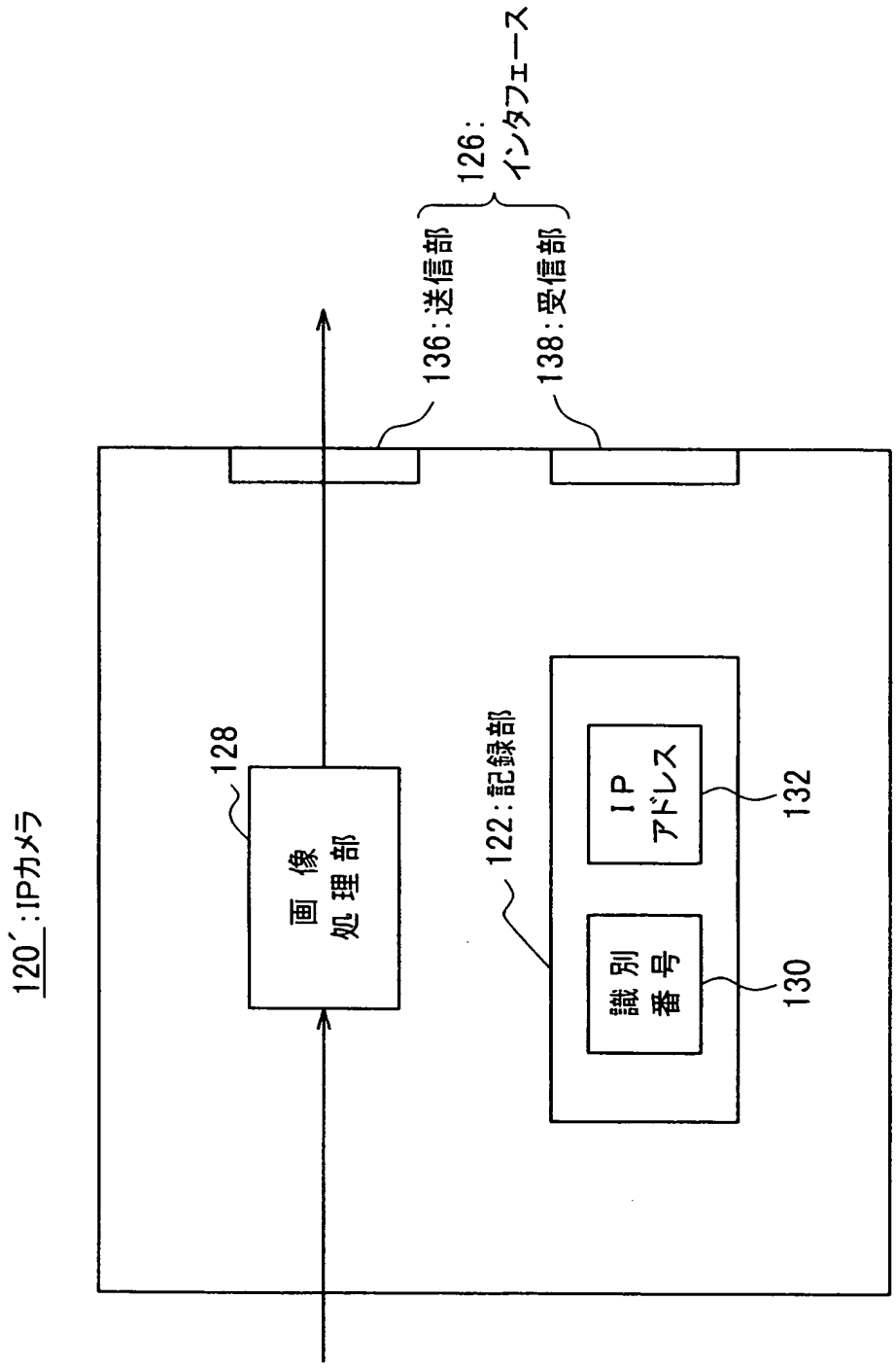
【図５】


500:認証サーバ
② 認証要求
400:閲覧装置
復号化
⑦ 閲覧
⑥ 復号化キー
④ 検出
⑤ 照合
300:メモリーカード
③ 送信
暗号化
100:撮像装置
① 撮像

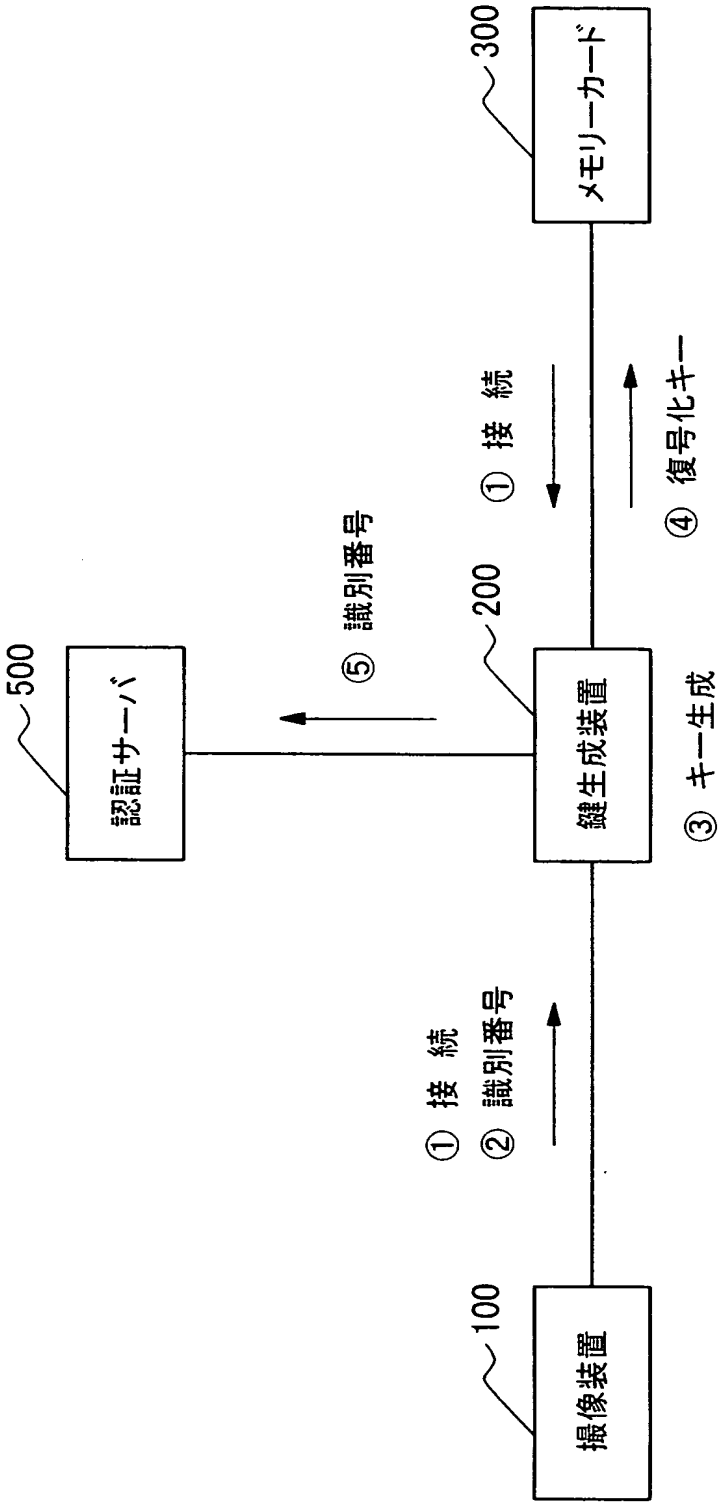
【図６】


開　始
撮像装置100による撮像、画像の暗号化
S201
閲覧装置400から認証サーバ500に認証要求
S202
認証サーバ500が撮像装置100を認証
S203
閲覧装置400がメモリーカード300を検出
S204
閲覧装置400が，メモリーカード300の識別番号と撮像装置100の識別番号との照合
S205
暗号化された画像を復号化キーで復号
S206
閲覧装置400での画像の閲覧
S207
終　了

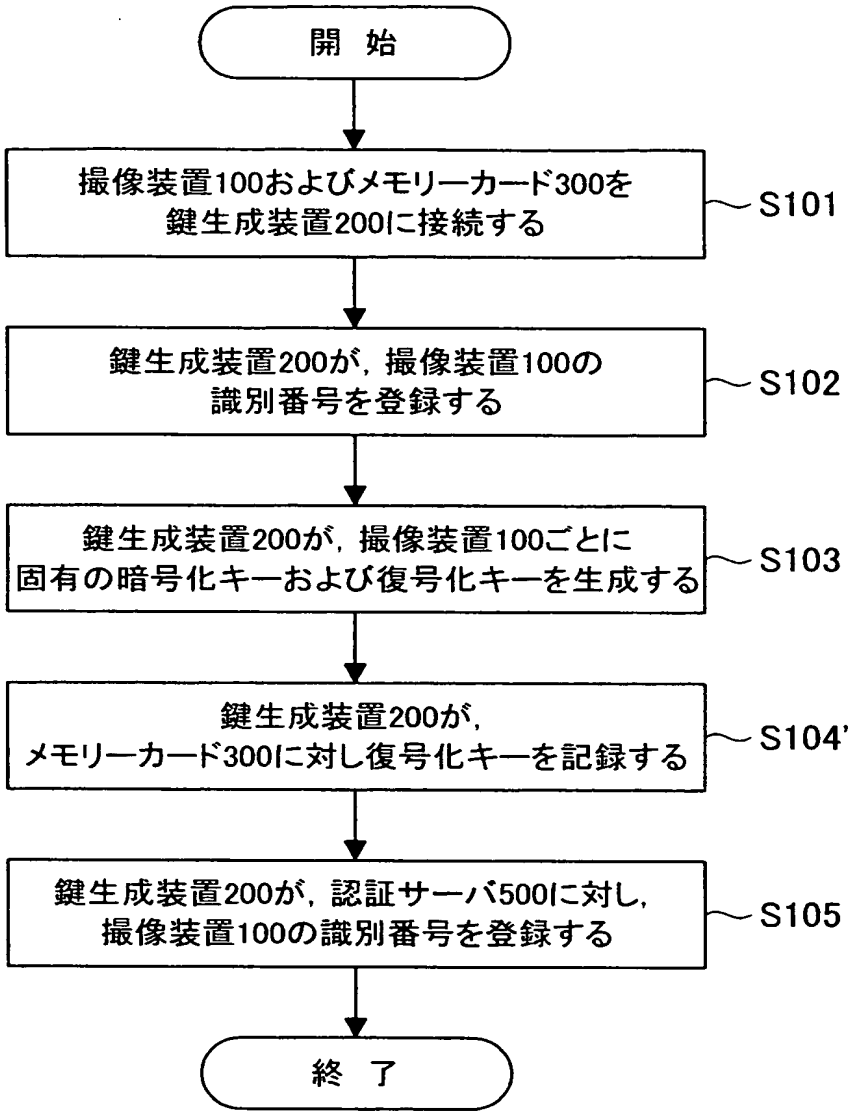
【図７】


120′:IPカメラ
126:
インタフェース
136:送信部
138:受信部
128
画像
処理部
122:記録部
IP
アドレス
132
識別
番号
130

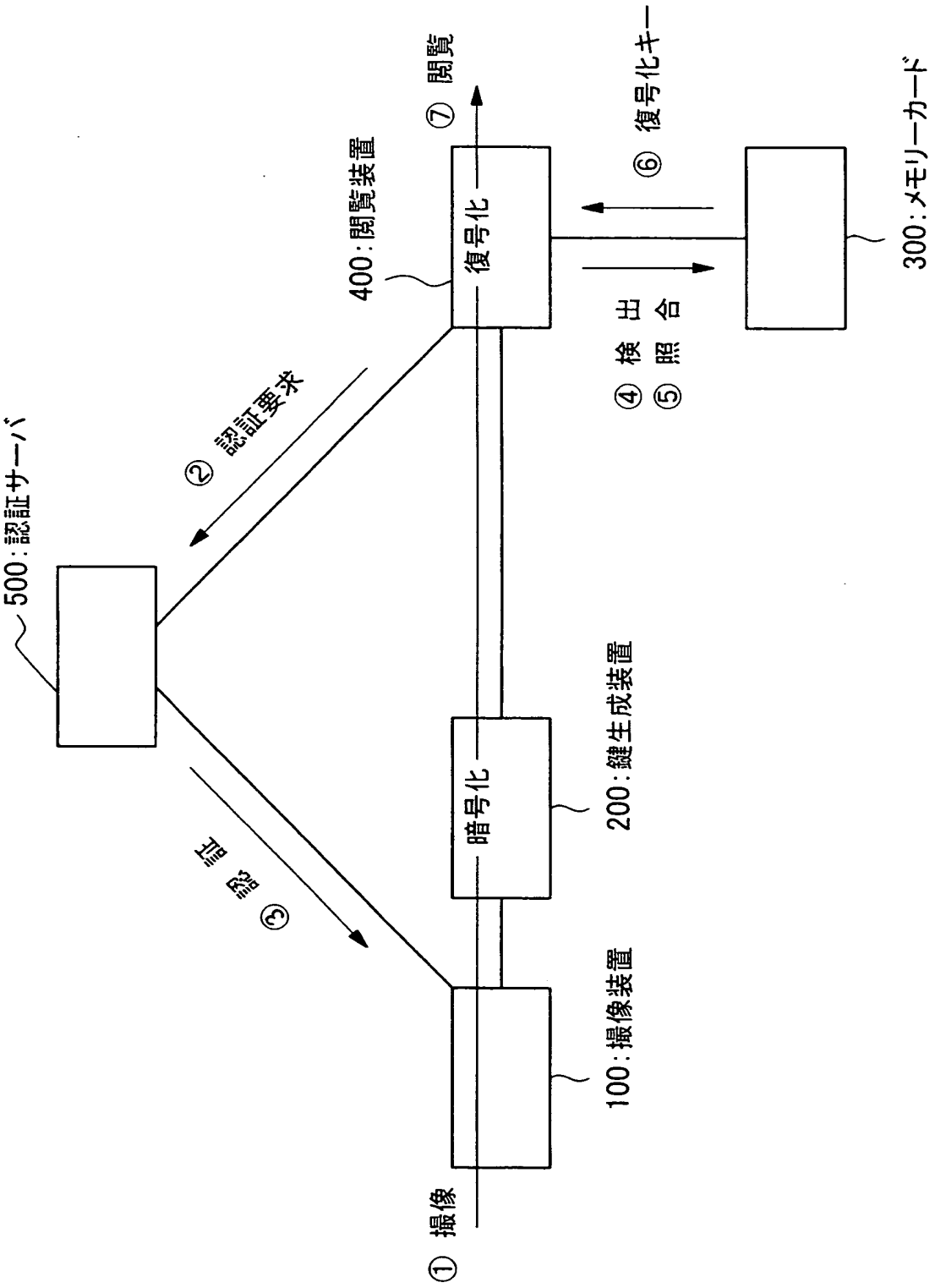
【図８】


300
メモリーカード
① 接 続
④ 復号化キー
200
鍵生成装置
③ キー生成
⑤ 識別番号
500
認証サーバ
① 接 続
② 識別番号
100
撮像装置

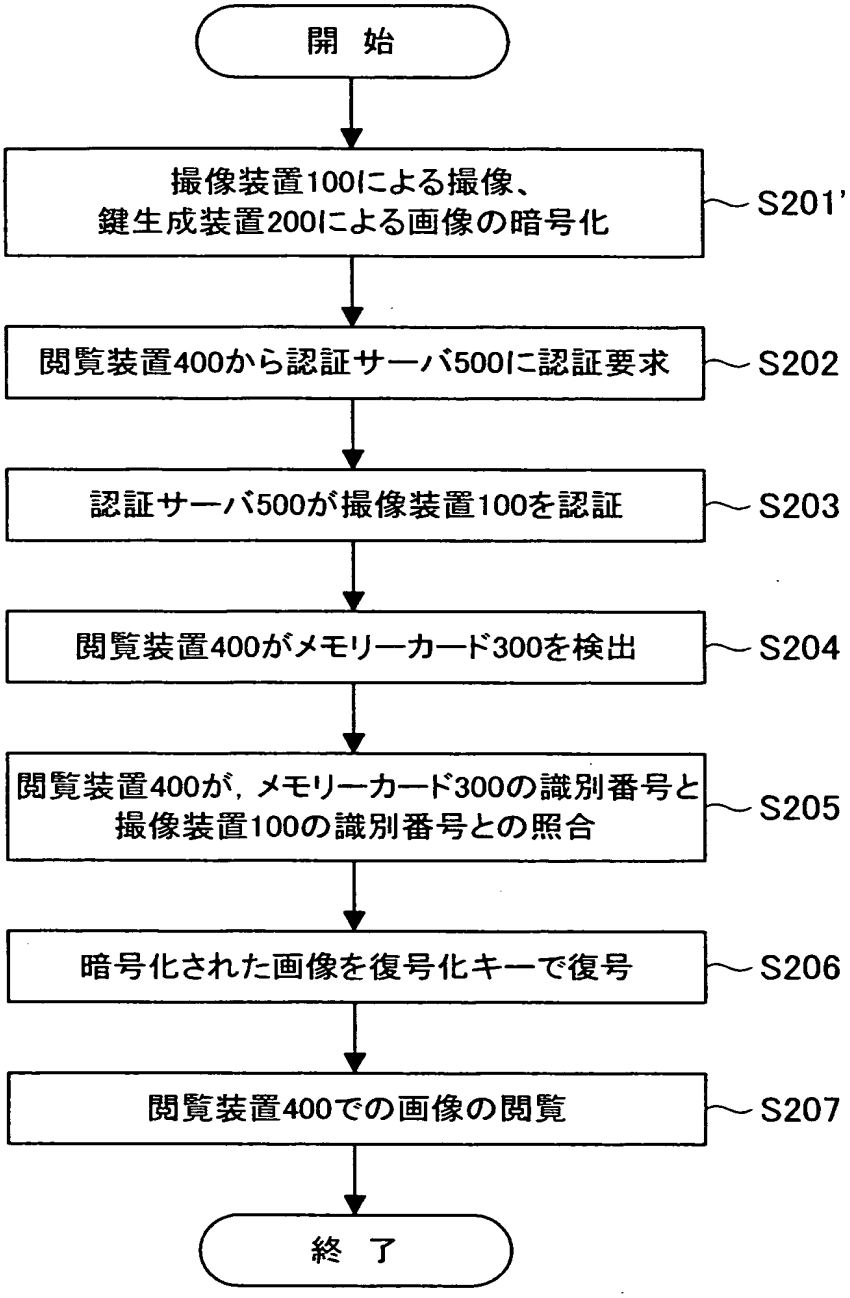
【図９】


開　始
撮像装置100およびメモリーカード300を
鍵生成装置200に接続する
S101
鍵生成装置200が，撮像装置100の
識別番号を登録する
S102
鍵生成装置200が，撮像装置100ごとに
固有の暗号化キーおよび復号化キーを生成する
S103
鍵生成装置200が，
メモリーカード300に対し復号化キーを記録する
S104'
鍵生成装置200が，認証サーバ500に対し，
撮像装置100の識別番号を登録する
S105
終　了

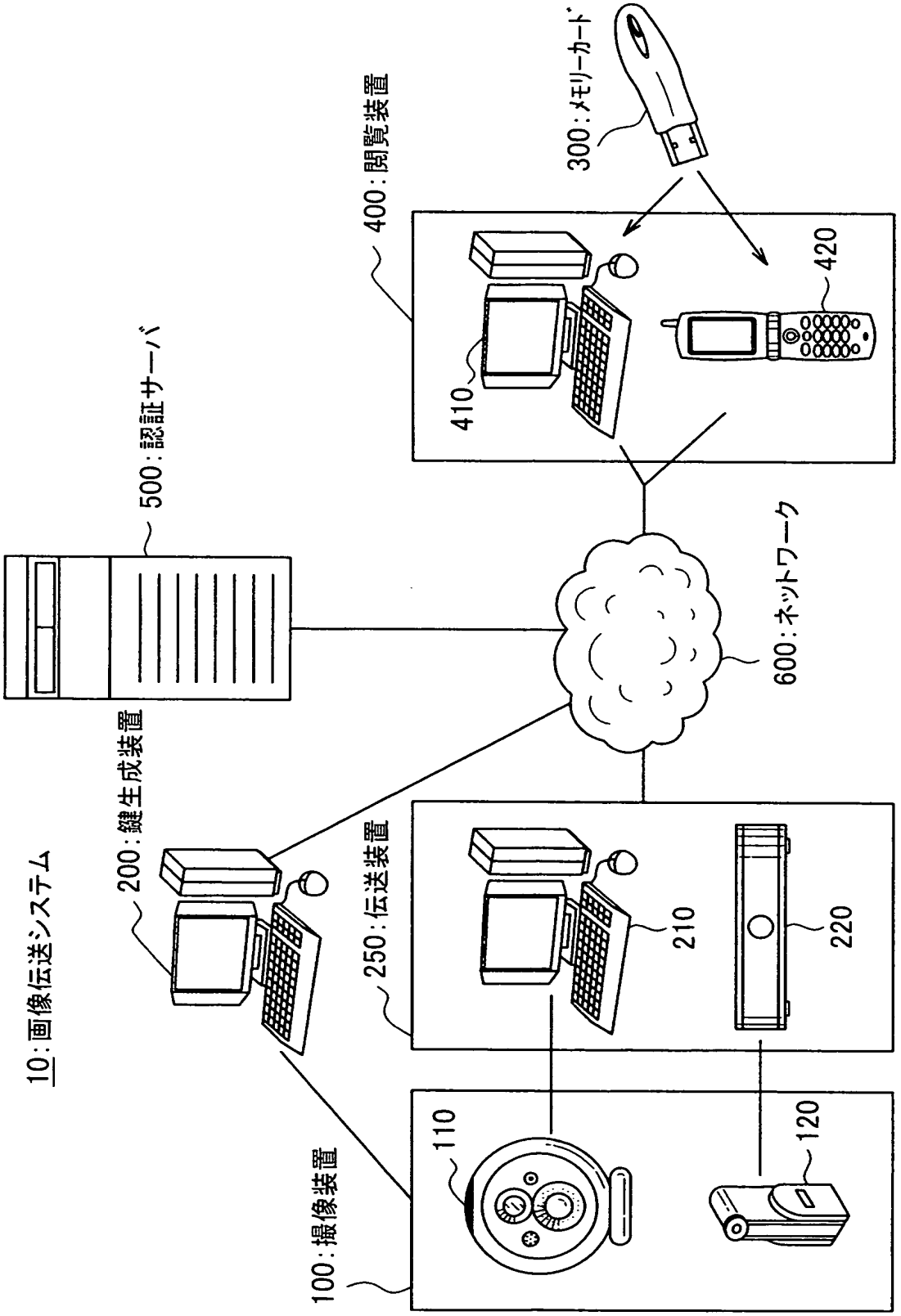
【図１０】


500:認証サーバ
② 認証要求
400:閲覧装置
復号化
⑦ 閲覧
⑥ 復号化キー
④ 検出
⑤ 照合
300:メモリーカード
暗号化
200:鍵生成装置
③ 送信
100:撮像装置
① 撮像

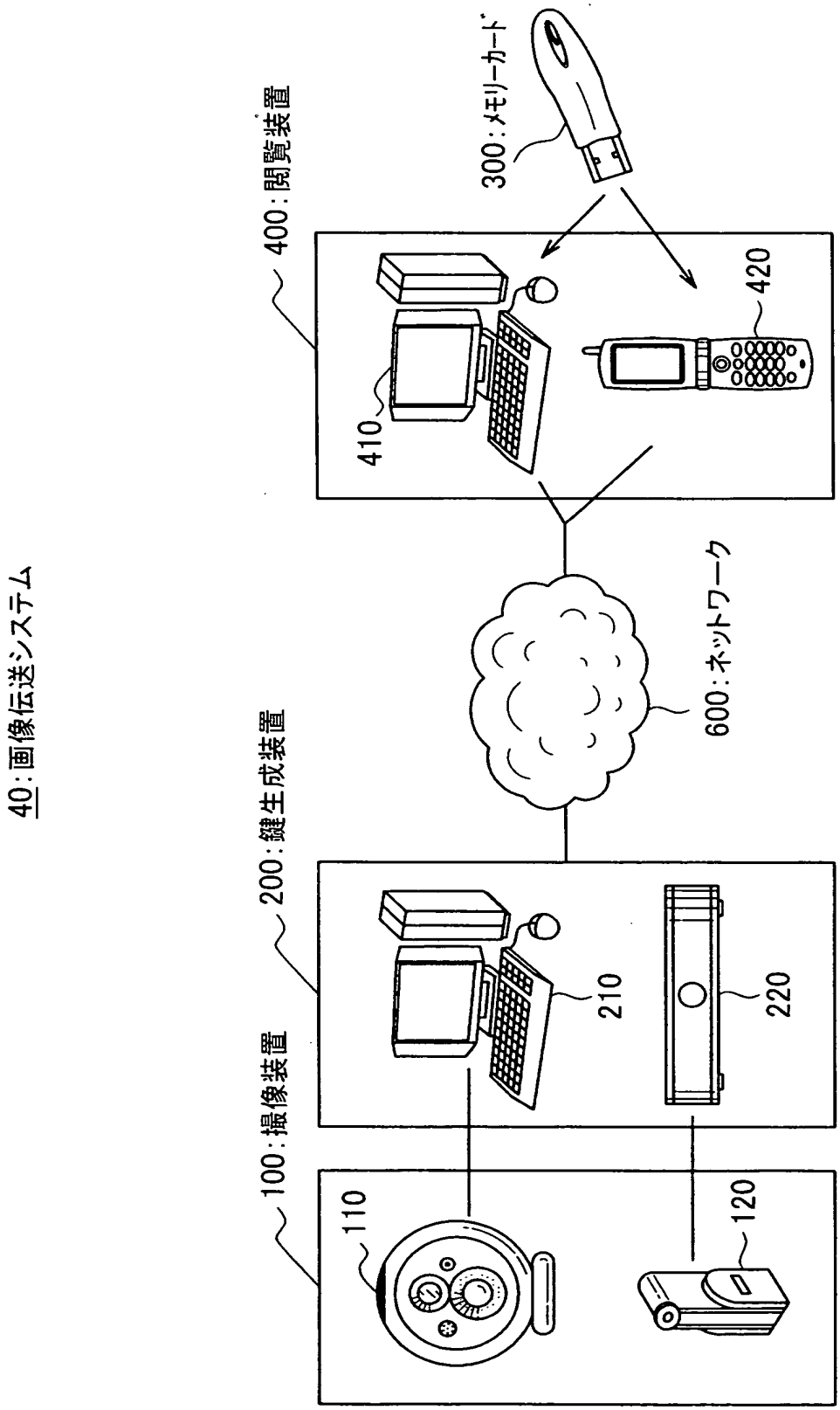
【図１１】


開　始
撮像装置100による撮像、
鍵生成装置200による画像の暗号化
S201'
閲覧装置400から認証サーバ500に認証要求
S202
認証サーバ500が撮像装置100を認証
S203
閲覧装置400がメモリーカード300を検出
S204
閲覧装置400が，メモリーカード300の識別番号と
撮像装置100の識別番号との照合
S205
暗号化された画像を復号化キーで復号
S206
閲覧装置400での画像の閲覧
S207
終　了

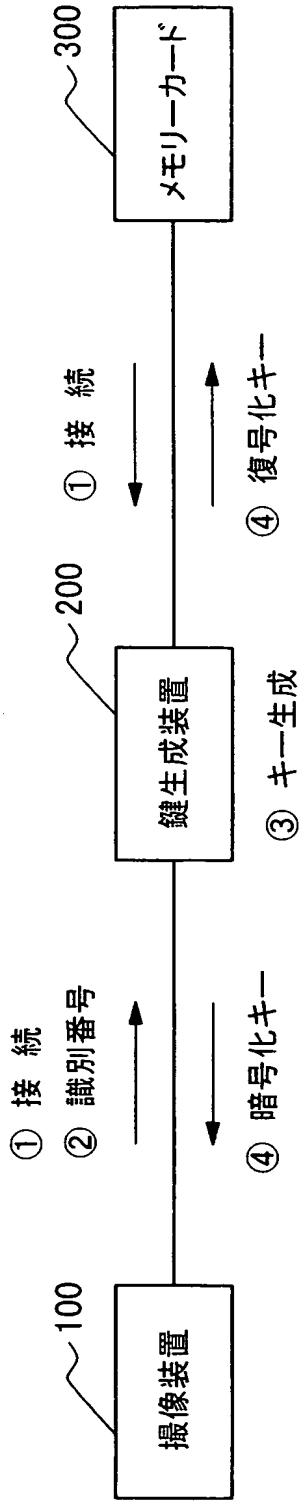
【図１２】


10:画像伝送システム
100:撮像装置
110
120
200:鍵生成装置
250:伝送装置
210
220
500:認証サーバ
600:ネットワーク
400:閲覧装置
410
420
300:メモリーカード

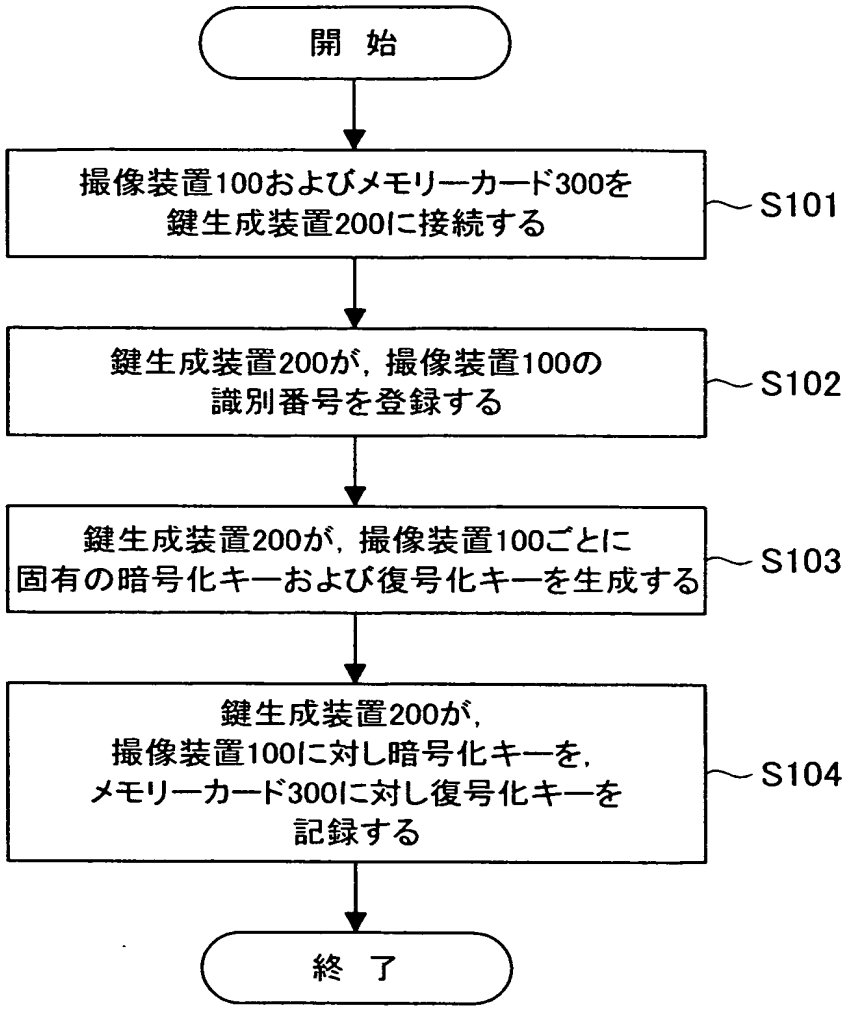
【図１３】


40:画像伝送システム
100:撮像装置
110
120
200:鍵生成装置
210
220
600:ネットワーク
400:閲覧装置
410
420
300:メモリーカード

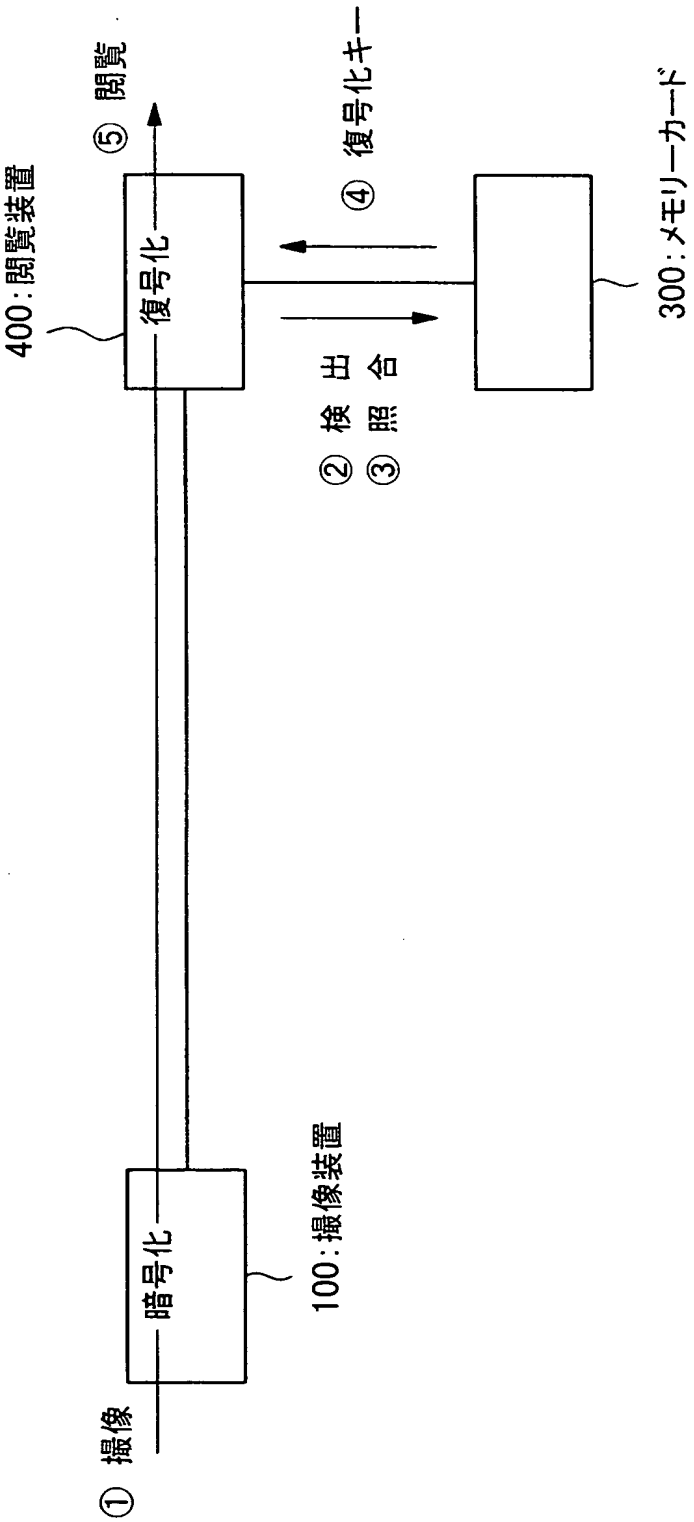
【図１４】


300
メモリーカード
① 接 続
④ 復号化キー
200
鍵生成装置
③ キー生成
① 接 続
② 識別番号
④ 暗号化キー
100
撮像装置

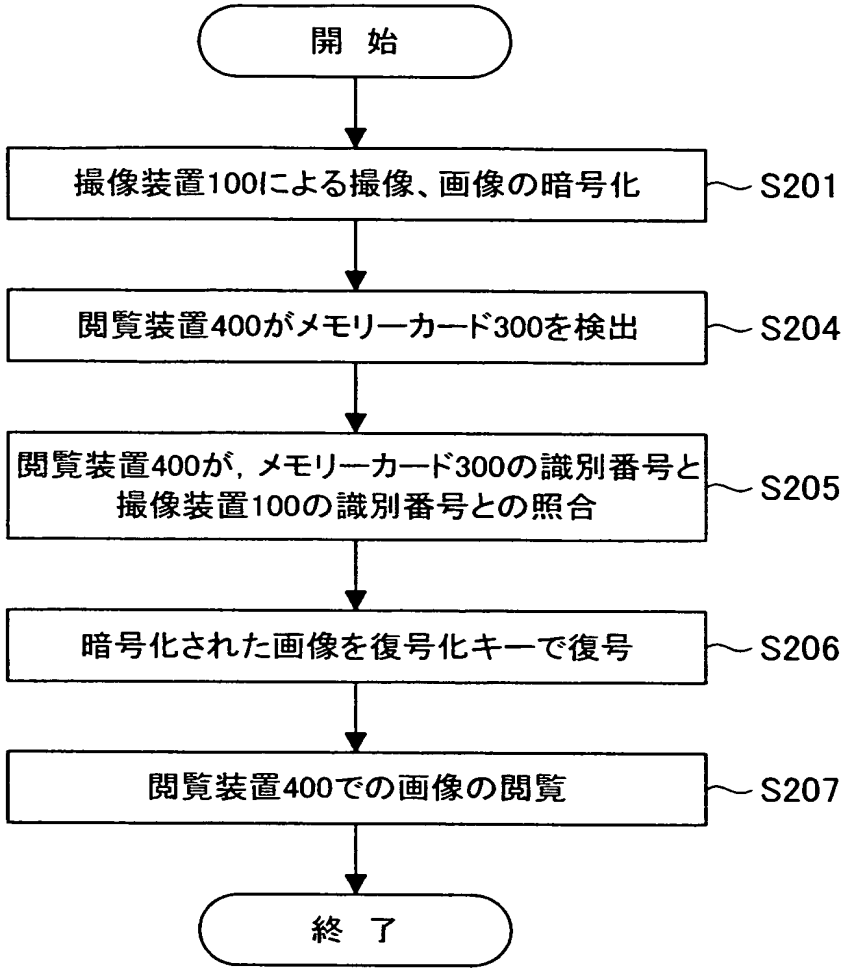
【図１５】


開　始
撮像装置100およびメモリーカード300を
鍵生成装置200に接続する
S101
鍵生成装置200が，撮像装置100の
識別番号を登録する
S102
鍵生成装置200が，撮像装置100ごとに
固有の暗号化キーおよび復号化キーを生成する
S103
鍵生成装置200が，
撮像装置100に対し暗号化キーを，
メモリーカード300に対し復号化キーを
記録する
S104
終　了

【図１６】



【図１７】


開　始
撮像装置100による撮像、画像の暗号化
S201
閲覧装置400がメモリーカード300を検出
S204
閲覧装置400が，メモリーカード300の識別番号と撮像装置100の識別番号との照合
S205
暗号化された画像を復号化キーで復号
S206
閲覧装置400での画像の閲覧
S207
終　了

【書類名】　要約書

【要約】

【課題】　他者に見られたくない画像をネットワーク経由で送出するにあたり，本人のみが安全に画像を見ることの可能な，画像伝送システムを提供する。

【解決手段】　画像伝送システム１０は，各々が固有の識別番号を有し，撮像した画像を暗号化してネットワークに伝送するための暗号化機能を有する１または２以上の撮像装置１００と，画像を暗号化するための暗号化キーおよび暗号化された画像を復号化するための復号化キーを撮像装置ごとに生成する鍵生成装置２００と，復号化キーと撮像装置の識別番号とを関連付けて記録するメモリーカード３００と，メモリーカードが接続され，復号化キーを用いて暗号化された画像を復号化する復号化機能を有し，ネットワークを介して撮像装置が伝送する画像を閲覧するための閲覧装置４００と，閲覧装置からアクセス可能な撮像装置の認証を行う認証サーバ５００を含む。

【選択図】　図１

特願２００３－１０１７８３

出　願　人　履　歴　情　報

識別番号　［０００００２１８５］

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社